McAfee
An Intel Company

Product Guide
Revision E

McAfee Data Loss Prevention 9.3.0

For use with ePolicy Orchestrator 4.5, 4.6, 5.0 Software

COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface **13**
About this guide . . . 13
Audience . . . 13
Conventions . . . 13
Find product documentation . . . 14

1 Introduction to McAfee Data Loss Prevention **15**
Understanding McAfee DLP products . . . 15
McAfee DLP product suite . . . 15
McAfee DLP data vectors . . . 16
How McAfee DLP works . . . 16
How McAfee DLP handles data . . . 16
How McAfee DLP acts on data . . . 19
Integrating multiple McAfee DLP products . . . 20

Deployment

2 Deployment options **25**
Types of installations . . . 25
Management options . . . 25
Using McAfee DLP with other McAfee products . . . 26

3 Deployment scenarios **27**
Deployment scenario: McAfee DLP Monitor . . . 27
Deployment scenario: McAfee DLP Discover and McAfee DLP Prevent . . . 28
Deployment scenario: Full product suite integration . . . 29

4 Plan your deployment **31**
Product-specific requirements . . . 31
Network integration requirements for McAfee DLP Monitor . . . 31
Requirements for configuring MTA servers with McAfee DLP Prevent . . . 33
Supported repositories with McAfee DLP Discover . . . 33
Network placement . . . 34
Default ports used in McAfee DLP communications . . . 34
Order of deployment . . . 36
Deployment Checklist . . . 37

Installation

5 Set up the hardware **41**
Check the shipment . . . 41
Rack mount the appliance . . . 41
Identify network ports . . . 42
Configure SPAN or tap mode for McAfee DLP Monitor . . . 43

Integrate the appliance using a SPAN port . . . 43
Integrate the appliance using a network tap . . . 43
Connect the management port . . . 44

6 Install or upgrade the system 45
Installing or upgrading the software on 4400 and 5500 appliances . . . 45
Download the 4400 or 5500 archive . . . 45
Install a new image on 4400 or 5500 appliances . . . 46
Upgrading appliances in a managed environment . . . 47
Upgrade the products on 4400 or 5500 appliances . . . 47
Boot options . . . 49
Set the next boot image . . . 50
Installing or upgrading the software on 1650 and 3650 appliances . . . 50
Download the 1650 or 3650 archive . . . 50
Install a new image on 1650 or 3650 appliances . . . 51
Upgrading appliances in a managed environment . . . 52
Upgrade the products on 1650 or 3650 appliances . . . 52
Applying hotfixes . . . 54
Re-imaging an appliance . . . 54

7 Complete post-installation tasks 55
Configure McAfee DLP Manager . . . 55
Add McAfee DLP Manager to ePolicy Orchestrator . . . 56
Install the network extension . . . 56
Add an ePolicy Orchestrator database user . . . 56
Register McAfee DLP Manager on ePolicy Orchestrator . . . 56
Install the host extension . . . 57
Required ePolicy Orchestrator registration information . . . 57
Register ePolicy Orchestrator on McAfee DLP Manager . . . 58
Add McAfee DLP devices to McAfee DLP Manager . . . 58
Configure standalone McAfee DLP appliances using the Setup Wizard . . . 59
Configure servers for McAfee DLP Prevent . . . 60
Link negotiation for McAfee DLP appliances . . . 60
Testing the system . . . 61
Additional tasks . . . 61

System configuration

8 Integrating network servers 65
Using external authentication servers . . . 65
OpenLDAP and Active Directory server differences . . . 65
How directory server accounts are accessed . . . 65
How directory servers are used with DLP systems . . . 66
How LDAP user accounts are monitored . . . 66
Monitoring LDAP users . . . 67
Add Active Directory servers . . . 67
Add Active Directory or OpenLDAP users . . . 69
Export certificates from Active Directory servers . . . 69
How ADAM servers extend McAfee DLP Manager . . . 70
Mapping default to custom attributes . . . 70
Using Active Directory attributes . . . 71
Viewing Active Directory incidents . . . 71
Search for user attributes in LDAP data . . . 72
Find user attributes in LDAP data . . . 72
LDAP columns available for display . . . 73
Add columns to display user attributes . . . 73

Using McAfee Logon Collector . . . 74
Connect McAfee Logon Collector to McAfee DLP Manager . . . 74
How McAfee Logon Collector enables user identification . . . 75
How McAfee DLP uses SIDs . . . 75
Using DHCP servers . . . 75
Add DHCP servers to DLP systems . . . 76
Using NTP servers . . . 76
Correct time in the McAfee DLP Manager interface . . . 76
Synchronize McAfee DLP devices with NTP servers . . . 77
Reset time manually . . . 78
Using syslog servers . . . 78

9 Administrator accounts 81
Managing user accounts . . . 81
Configure primary administrator accounts . . . 81
Activate a failover account . . . 82
Customize logon settings . . . 82
Customize password settings . . . 82
Managing user groups . . . 83
Add user groups . . . 83
Delete user groups . . . 84
Managing permissions . . . 84
Assign incident permissions . . . 84
Assign task and policy permissions . . . 85
Check user permissions . . . 85
Check group incident permissions . . . 85

Policy configuration and data use

10 Policies and rules 89
How policies and rules can be used . . . 89
Analyzing trends in data matching . . . 89
Use Chart and Compare to prioritize policies . . . 90
Use Chart and Compare to tune policies and rules . . . 90
Managing policies . . . 91
Policy inheritance . . . 91
Policy activation . . . 92
Activate or deactivate policies . . . 92
Add, modify, and deploy policies . . . 92
Managing rules . . . 96
Add rules . . . 97
Find rules . . . 97
View rule parameters . . . 98
Copy rules to policies . . . 98
Disable rule inheritance . . . 99
Reconfigure rules for web traffic . . . 99
Delete rules . . . 100
Modify rules . . . 100
Refining rules . . . 100
Tune rules . . . 100
Identify false positives . . . 102
Define exceptions . . . 102
Add new rules with exceptions . . . 103
Typical scenarios . . . 103
Protect intellectual property by customizing a standard policy . . . 103
Identify insider threats by deploying a standard policy . . . 104

Block data containing source code . . . 105
Block transmission of financial data . . . 105
Modify alphanumeric patterns in rules that produce false positives . . . 106
Track intellectual property violations . . . 107

11 Rule elements 109

Action rules . . . 109
How McAfee DLP Prevent uses action rules . . . 110
How McAfee DLP Endpoint uses action rules . . . 110
How McAfee DLP Discover uses action rules . . . 111
Add, modify, or delete action rules . . . 112
Concepts . . . 117
Types of concepts . . . 117
How content concepts work . . . 117
Regular expression syntax for concepts . . . 117
Add, apply, restore, and delete concepts . . . 118
Typical scenarios . . . 123
Templates . . . 124
How templates work . . . 125
Add, modify, and delete templates . . . 126
Typical scenarios . . . 127
Content types . . . 129
Advanced documents content types . . . 129
Apple application content types . . . 130
Binary content types . . . 130
Chat content types . . . 130
Compressed and archive formats . . . 130
Desktop content types . . . 131
Engineering drawing and design content types . . . 131
Executable content types . . . 132
Image content types . . . 132
Language classification content types . . . 132
Mail content types . . . 133
Microsoft content types . . . 133
Multimedia content types . . . 134
Office application content types . . . 134
Peer-to-peer content types . . . 135
Protocol content types . . . 135
Source code content types . . . 136
Unclassified content types . . . 136
UNIX content types . . . 137

12 Policy configuration options 139

Policy definition options . . . 139
Rule options . . . 140
Action rule options . . . 140
Template options . . . 141
Concept options . . . 142
Document property options . . . 142
Registered document options . . . 143
Policy setting options . . . 143

13 Integrating McAfee DLP Endpoint 145

How McAfee DLP Endpoint works with McAfee DLP Manager . . . 145
Setting up McAfee DLP Endpoint . . . 146
Installing McAfee DLP Endpoint . . . 146

Configure McAfee Agent on ePolicy Orchestrator . . . 147
Add an evidence folder on ePolicy Orchestrator . . . 147
Configuring McAfee DLP Endpoint on McAfee DLP Manager . . . 148
Working with a unified policy . . . 151
Unified policy content strategy . . . 151
Integration into the unified workflow . . . 152
How McAfee DLP Endpoint rules are mapped . . . 152
Adding endpoint parameters to rules in McAfee DLP Manager . . . 152
Using protection rules in McAfee DLP Manager . . . 154
Extending McAfee DLP Discover scans to endpoints . . . 155
Applying tags by scanning . . . 155
How signatures used at endpoints are stored . . . 155
Scanning local drives . . . 156
Tagging and tracking . . . 157
Using tags . . . 157
Application-based tagging . . . 158
Location-based tagging . . . 165
Controlling devices . . . 167
Device classes . . . 168
Classifying devices . . . 168
Controlling devices with device definitions . . . 170
Using device rules . . . 173
Device parameters . . . 176
Working with endpoint events . . . 178
View endpoint events . . . 178
Events reported to McAfee DLP Manager . . . 178
Typical scenarios . . . 179
Keep data from being copied to removable media . . . 179
Keep data from being cut and pasted . . . 180
Protect data with Document Scan Scope . . . 181
Keep data from being printed to file . . . 181
Protect data from screen capture . . . 182
Protect data by identifying text in title bars . . . 183
Keep data from being printed on network printers . . . 184
Create user list templates to control access . . . 185
Keep data from being printed on local printers . . . 185
Protect data using specific encryption types . . . 186

14 Scanning databases and file repositories 189

Types of scans . . . 189
Supported repositories with McAfee DLP Discover . . . 190
Scanning network attached storage . . . 190
Firewall options for scanning . . . 191
Scanning databases . . . 191
Database terminology . . . 192
How database content is registered . . . 192
Database filtering options . . . 193
Using SSL certificates . . . 196
Scanning file repositories . . . 198
How McAfee DLP Discover uses OLAP . . . 198
How the classification engine works . . . 199
How data classification scans work . . . 200
How classified data is displayed . . . 200
Creating optimized scans from the Task View page . . . 201
Registering documents and structured data . . . 202
Types of signatures . . . 203

How signatures are shared with managed systems . . . 204
Upload documents and data for registration . . . 205
Reconfigure Firefox 3.5.x to view complete paths . . . 205
Exclude text from registration . . . 206
Unregister content . . . 206
Re-register content . . . 207
Managing scans . . . 207
Preparing to scan . . . 207
Configuring Microsoft SharePoint scans . . . 208
Defining scans . . . 208
Using credentials to authorize entry . . . 215
Scheduling scans . . . 217
Scan states . . . 218
Managing scan load . . . 221
McAfee DLP Discover scan permissions . . . 222
McAfee DLP Discover registration permissions . . . 223
Managing discovered files . . . 224
Types of remedial actions . . . 224
Compliance with FIPS standards . . . 225
Review remedial actions . . . 225
Add columns to display remedial actions . . . 225
Add remedial action rules . . . 226
Apply remedial action rules . . . 226
Set up locations for exported files . . . 227
Copy discovered files . . . 227
Move discovered files . . . 228
Encrypt discovered files . . . 229
Delete discovered files . . . 230
Revert remediated files . . . 230
Scan statistics and reports . . . 231
View scan results . . . 231
View the list of scanned files . . . 232
Export reports of scan statistics . . . 232
Get historical scan statistics . . . 233
Types of task status messages . . . 233
Types of system status messages . . . 234
Typical scenarios . . . 235
Scheduling lengthy scans to run at regular intervals . . . 235
Create a one-time scan that runs until it completes . . . 235
Create a scan that runs only when started manually . . . 237
Identify and track sensitive documents . . . 237
Control copies of sensitive documents . . . 238

15 Incident dashboards and reports 239

Using the Home page . . . 239
Customize the Home page . . . 240
Assign Home page permissions . . . 240
Managing incidents . . . 241
Sort incidents . . . 241
Filter incidents . . . 242
Getting incident details . . . 244
Set up incident views . . . 246
Customizing dashboards . . . 249
Expand dashboard displays . . . 249
Add rows to the dashboard . . . 249
Configure dashboard columns . . . 249

Add a match string column . . . 250
Controlling dashboard settings . . . 250
Troubleshooting dashboard incidents . . . 251
Generating reports . . . 252
Create PDF reports . . . 252
Create HTML reports . . . 252
Create CSV reports . . . 253
Schedule reports . . . 253
Add titles to reports . . . 254
Add custom logos to reports . . . 254
Typical scenarios . . . 255
Find policy violations by user . . . 255
Find high-risk incidents . . . 256

16 Case management 257
Managing cases . . . 257
Add, delete, or save cases . . . 258
Manage case permissions . . . 260
Updating cases . . . 261
Change ownership of a case . . . 261
Change status of a case . . . 261
Change the priority of a case . . . 261
Change the resolution stage of a case . . . 262
Add notes to a case . . . 262
Customizing cases . . . 262
Add or remove attachments to cases . . . 262
Add or remove custom case attributes . . . 263
Customize Case List columns . . . 264
Customize case notifications . . . 264
Notify stakeholders of case updates . . . 264
Typical scenario . . . 265
Resolve credit card violations using a case . . . 265

17 Searching captured data 267
How McAfee DLP handles searching . . . 267
Distributed searching . . . 267
Large-scale searches . . . 268
Number of results supported . . . 268
Archive handling . . . 268
Case insensitivity . . . 268
Microsoft Office 2007 anomalies . . . 268
Negative searches . . . 269
Proper name treatment . . . 269
Parts of speech excluded from capture . . . 269
Special character exceptions . . . 269
Word stemming . . . 270
Search basics . . . 270
Add or delete parameters . . . 271
Retrieve data from directory servers . . . 271
Get search details . . . 272
View search results . . . 272
Stop searching . . . 272
Set up notification for backgrounded queries . . . 273
Clone searches . . . 273
Using logical operators in searches . . . 273
Logical operators supported in queries . . . 274

Examples of queries using logical operators . . . 274
Using keywords in searches . . . 275
Using keywords to find incidents . . . 275
Find incidents using keywords . . . 276
Find incidents by excluding keywords . . . 276
Find exact keyword matches . . . 276
Find non-English keywords . . . 277
Build keyword expressions with logical operators . . . 277
Using concepts in searches . . . 278
Find incidents using content concepts . . . 278
Build concept expressions with logical operators . . . 278
Exclude concepts to filter results . . . 279
Search based on network parameters . . . 280
Search using time parameters . . . 280
Search by port . . . 282
Search by port range . . . 282
Search by excluding ports . . . 283
Common port assignments . . . 283
Search by using protocols . . . 284
Search by excluding protocols . . . 284
Find incidents related to geographic locations and web sites . . . 285
Find IP addresses in incidents . . . 285
Search for email . . . 287
Search based on file parameters . . . 293
Finding document properties in context . . . 294
Find files by signature . . . 295
Find common names in different organizational units . . . 295
Find files by size . . . 296
Find files by type . . . 296
Find document types . . . 297
Find Microsoft or Apple documents . . . 297
Find office documents . . . 298
Find proprietary documents . . . 298
Find files with human imagery . . . 299
Find images using file types . . . 299
Search discovered data . . . 299
Typical scenarios . . . 306
Find leaked documents . . . 306
Monitor sensitive files after close of business in different time zones . . . 307
Find email using non-standard ports . . . 307
Find evidence of frequent communications . . . 308
Find source code leaving the network . . . 309
Find encrypted traffic and files . . . 309
Find unencrypted user data . . . 310
Find geographic users and incidents . . . 310
Find evidence of foreign interference . . . 310
Search for social networking activity . . . 311
Find postings to message boards . . . 311
Find frequently visited web sites . . . 312

18 Capture filters 313
How capture filters work . . . 313
Types of capture filters . . . 313
How content capture filters work . . . 314
How network capture filters work . . . 315
Manage capture filters . . . 316

Add content capture filters . . . 316
Add network capture filters . . . 317
Copy capture filters . . . 318
Deploy capture filters . . . 318
View deployed capture filters . . . 318
Remove deployed capture filters . . . 319
Reprioritize capture filters . . . 319
Modify capture filters . . . 320
Typical scenarios . . . 320
Filter out traffic using common IP addresses . . . 320
Manage data capture with network capture filters . . . 321
Exempt users from detection . . . 322

Maintenance

19 Managing McAfee DLP systems 327
Configure McAfee DLP system information . . . 327
Add McAfee DLP devices to McAfee DLP Manager . . . 328
Unregister McAfee DLP devices . . . 328
Restart McAfee DLP appliances or services . . . 329
Change link speed . . . 329
Manage McAfee DLP appliance disk space . . . 330
Setting wiping policies . . . 330
Monitoring audit logs . . . 330
Auditing live users . . . 330
SNMP management . . . 332
Configure SNMP on 4400 or 5500 appliances . . . 333
Configure SNMP on 1650, 3650, or virtual appliances . . . 334
Default SNMP v3 settings . . . 334
Using network statistics . . . 335
Types of network statistics . . . 335
Filtering network statistics . . . 335
Technical specifications . . . 336
McAfee DLP rack mounting requirements . . . 336
McAfee DLP power redundancy . . . 336
McAfee DLP FCC compliance . . . 336
McAfee DLP safety compliance guidelines . . . 337

20 Disaster recovery backup and restore 339
How the backup and restore process works . . . 339
What a backup contains . . . 339
Backup and restore considerations . . . 340
Restoring on different hardware . . . 341
Back up McAfee DLP systems . . . 341
Restore McAfee DLP systems . . . 342
Test a restored system . . . 343

21 Technical support 345
Contact technical support . . . 345
Create a technical support package . . . 345

Index 347

Preface

This guide provides the information you need to configure, use, and maintain McAfee® Data Loss Prevention.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction to McAfee Data Loss Prevention

McAfee® Data Loss Prevention (McAfee DLP) is a suite of products that identifies and protects data within your network.

Use McAfee DLP to understand what type of data is on your network. McAfee DLP allows you to determine how the data is being accessed and transmitted, to determine if the data is sensitive, and to implement effective protection policies while reducing the need for extensive trial and error, all from a single management console.

Contents

- *Understanding McAfee DLP products*
- *How McAfee DLP works*

Understanding McAfee DLP products

McAfee DLP offers several products to accommodate different types of data within your network.

McAfee DLP product suite

Five separate products make up the McAfee DLP product suite.

- **McAfee DLP Manager** — Provides centralized management of all your McAfee DLP products
- **McAfee DLP Monitor** — Captures and analyzes traffic flowing through your network
- **McAfee DLP Prevent** — Works with your web proxy or Mail Transfer Agent (MTA) server, protecting email and web traffic
- **McAfee DLP Discover** — Scans databases and file repositories to identify and protect sensitive data
- **McAfee DLP Endpoint** — Runs on endpoint devices to inspect and control user actions

McAfee DLP data vectors

McAfee DLP collects data and categorizes it in one of three vectors — *Data in Motion*, *Data at Rest*, and *Data in Use*.

Table 1-1 Data vector descriptions

Data vector	Description	Associated products
Data in Motion	Data in Motion applies to live traffic on your network. Traffic is analyzed, categorized, and stored in the McAfee DLP database.	• McAfee DLP Monitor • McAfee DLP Prevent
Data at Rest	Data at Rest applies to data residing in databases, file shares, and repositories. McAfee DLP can scan, track, and perform remedial actions on data at rest.	McAfee DLP Discover
Data in Use	Data in Use applies to the actions of users on endpoint devices, such as copying data and files to removable media, printing files to a local printer, and taking screen captures. These actions are monitored and can be prevented.	McAfee DLP Endpoint

How McAfee DLP works

McAfee DLP features a capture engine that collects, analyzes, and classifies data within a network.

Classified data is saved as objects in the McAfee DLP database. These objects contain a variety of attributes. These terms describe the workflow for using McAfee DLP to identify and protect your data.

- **Policies and rules** — Create policies and rules to identify data that matches specified attributes.
- **Incidents** — If data retrieved from the network, a repository, or an endpoint device matches the attributes in a rule, McAfee DLP generates an incident. Incidents are reported to the McAfee DLP dashboard.
- **Cases** — Group related incidents to a case. Assign cases to an administrator or a group of administrators for further analysis.
- **Capture filters** — Configure capture filters to filter out portions of data that does not require analysis, reducing the number of false positives and increasing the performance of the system.
- **Searches** — Search historical data, which can be used to create new policies and rules where necessary.

How McAfee DLP handles data

The McAfee DLP products handle data differently, depending on what the data is and where the data is on the network.

Monitoring data with McAfee DLP Monitor

McAfee DLP Monitor connects to either a Switched Port Analyzer (SPAN) port or a network tap to passively monitor live traffic.

McAfee DLP Monitor captures, analyzes, and stores data, but does not take any blocking or preventive actions. Data collected by McAfee DLP Monitor is used to determine who sends what kind of data through the network, and where the data is sent.

Placement of the appliance on the network determines the data that is captured. Typically, McAfee DLP Monitor is connected to the LAN switch before the WAN router.

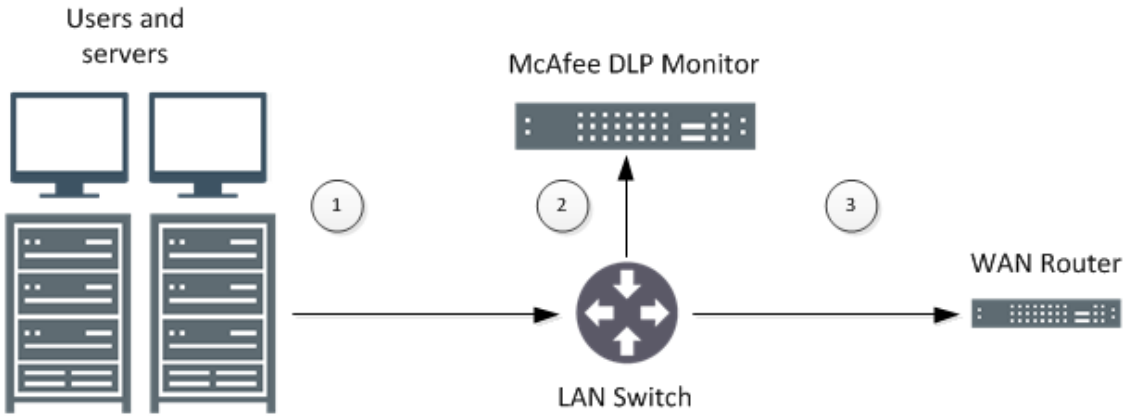


Figure 1-1 McAfee DLP Monitor traffic flow

1	The LAN switch receives network packets from internal users and servers.
2	McAfee DLP Monitor receives copies of network packets and analyzes them.
3	The switch sends packets to the WAN router. Packets sent from the WAN router to the switch will also be analyzed by McAfee DLP Monitor.

Protecting email and web traffic with McAfee DLP Prevent

McAfee DLP Prevent integrates with an MTA server or web proxy to monitor and act upon email and web traffic.

McAfee DLP Prevent does not support processing both web and email traffic on the same appliance.

McAfee DLP Prevent and email

McAfee DLP Prevent receives SMTP connections from an MTA server, analyzes email messages to detect policy violations, adds message headers to perform the configured action, and returns the message to the server.

Examples of actions taken on email traffic include:

- Blocking confidential data breaches
- Encrypting authorized transmissions
- Monitoring traffic, allowing email but still generating incidents
- Quarantining suspicious traffic
- Bouncing email that violates policies
- Notifying supervisory personnel
- Recording incidents in a system log

- Allowing email that is determined to be legitimate
- Redirecting email to other users or groups

McAfee DLP Prevent supports up to 30 concurrent SMTP connections. McAfee recommends configuring the MTA server to limit the number of connections to McAfee DLP Prevent to 25.

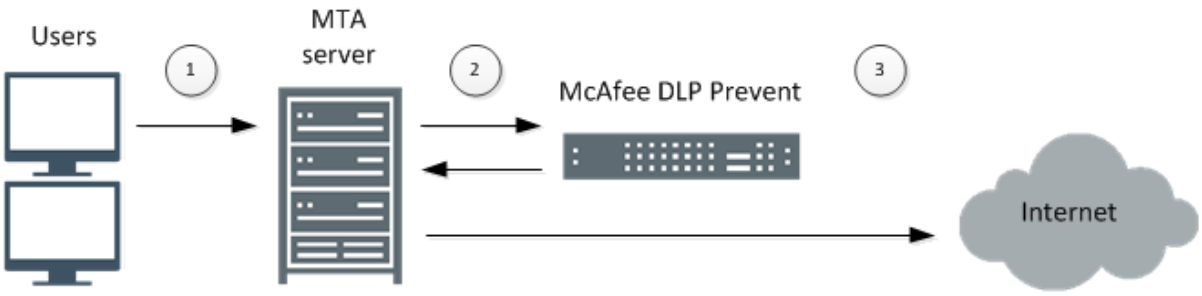


Figure 1-2 McAfee DLP Prevent email traffic flow

1	User email messages are sent to the MTA server.
2	The MTA server forwards the email messages to McAfee DLP Prevent. McAfee DLP Prevent inspects the email messages, adds appropriate headers, and sends the email messages back to the MTA server.
3	The MTA server sends the email messages to the appropriate destinations.

Some networks might have more than one email server that handles email messages that must be inspected. McAfee DLP Prevent can be configured to accept email messages from more than one MTA server. However, McAfee DLP Prevent forwards the inspected email messages to only one MTA server, known as the Smart Host.

McAfee DLP Prevent and web traffic

McAfee DLP Prevent receives ICAP connections from a web proxy server, analyzes the content, and determines if the traffic should be allowed or blocked.

McAfee DLP Prevent supports up to 4000 concurrent ICAP connections.

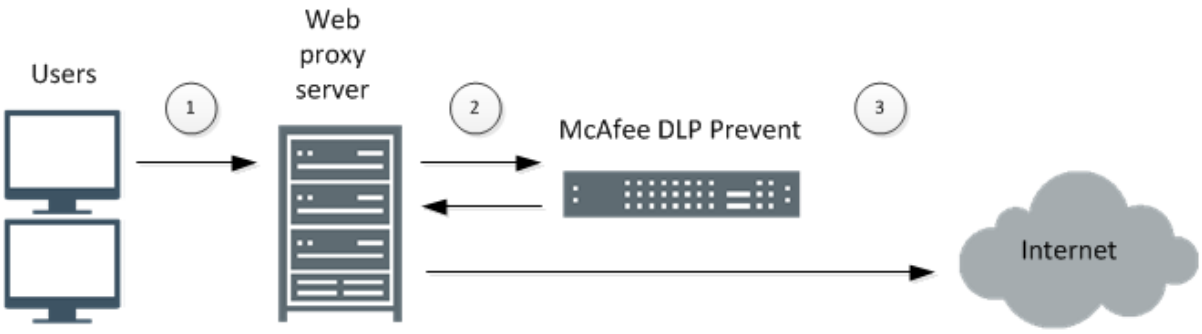


Figure 1-3 McAfee DLP Prevent web traffic flow

1	Users send web traffic to the web proxy server.
2	The web proxy server forwards the web traffic to McAfee DLP Prevent. McAfee DLP Prevent inspects the web traffic, adds appropriate headers, and sends the traffic back to the web proxy server.
3	The web proxy server sends the inspected web traffic to the appropriate destinations.

Scanning data and files with McAfee DLP Discover

McAfee DLP Discover scans databases and file repositories to identify sensitive data.

McAfee DLP Discover features different types of scans to retrieve the type and level of information you need. McAfee DLP Discover can perform a high-level scan, informing you of the number and types of files residing on a repository. In-depth scans analyze the entire contents of a database or set of files. McAfee DLP Discover can create signatures used to identify the same data or files on other repositories.

In a managed environment, sensitive data and files found by McAfee DLP Discover can be registered to McAfee DLP Manager. You can configure policies for other McAfee DLP devices to take action if sensitive files or data are accessed or transmitted across the network improperly.

Controlling user actions with McAfee DLP Endpoint

McAfee DLP Endpoint is software that runs on supported endpoint devices. McAfee DLP Endpoint inspects and controls users' activity.

Actions that McAfee DLP Endpoint can take include:

- Determine if a user is transmitting encrypted files
- Prevent copy and paste functionality
- Prevent a user from taking screen captures
- Prevent a user from transmitting files to removable media
- Scan a device file system to identify sensitive files or data
- Quarantine or delete files that are in violation of company policy

McAfee DLP Endpoint requires McAfee® ePolicy Orchestrator® (ePolicy Orchestrator) for management. McAfee DLP Manager is required to integrate McAfee DLP Endpoint with full McAfee DLP product suite.

If McAfee DLP Endpoint is the only McAfee DLP product you are deploying, see the *McAfee Data Loss Prevention Endpoint Product Guide* for installation and configuration instructions.

How McAfee DLP acts on data

Depending on the product, you can take preventive or corrective actions in the event of a policy violation.

Table 1-2 McAfee DLP actions by product

Product	Data vector	Action
McAfee DLP Monitor	Data in Motion	Allow
McAfee DLP Prevent	Data in Motion	**In use with a proxy server**: • Block • Monitor **In use with an MTA server**: • Block • Bounce • Encrypt • Monitor • Notify • Quarantine • Redirect

Table 1-2 McAfee DLP actions by product *(continued)*

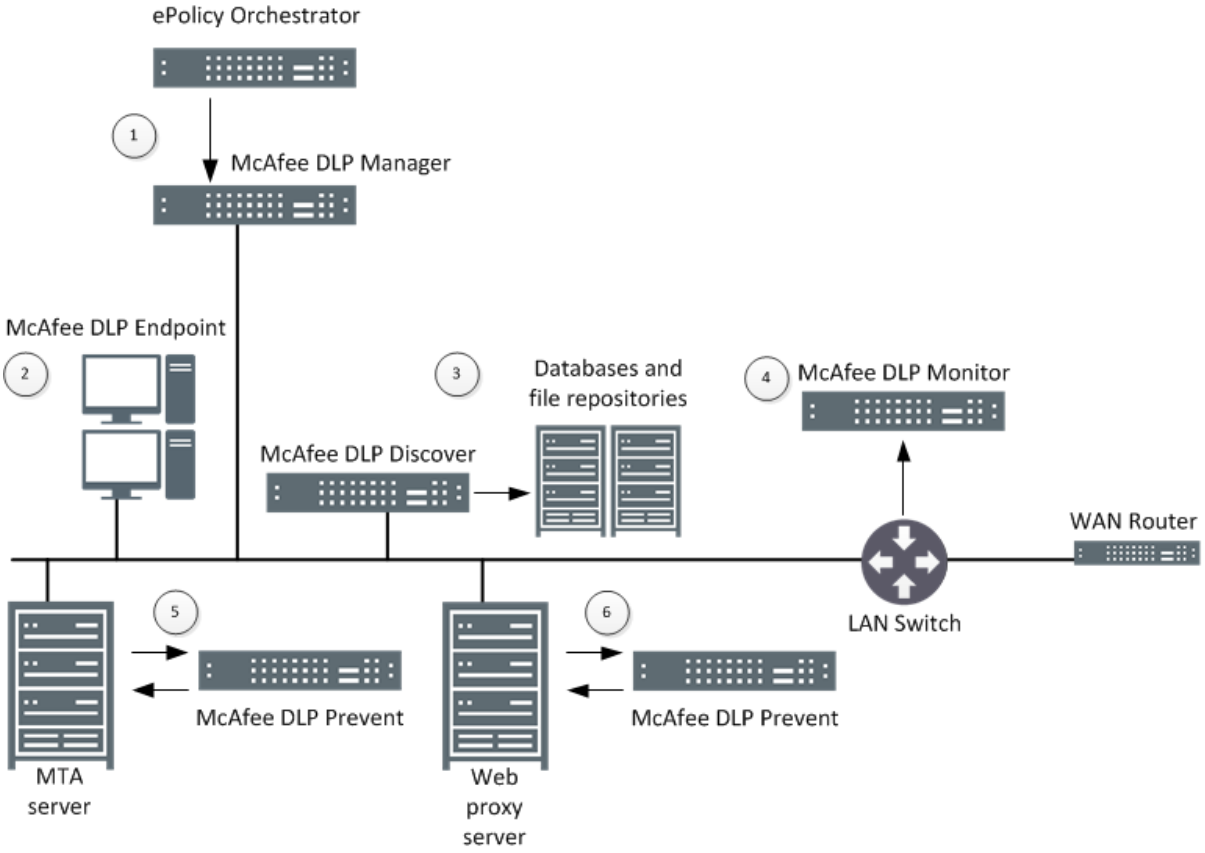
Product	Data vector	Action
McAfee DLP Discover	Data at Rest	• Move • Copy • Encrypt • Delete
McAfee DLP Endpoint	Data in Use	• Block • Delete • Encrypt • Monitor • Notify • Quarantine • Request Justification • Store Evidence • Tag

Integrating multiple McAfee DLP products

The McAfee DLP products can fully integrate to utilize the full feature set of the product suite.

Example: You configure McAfee DLP Discover to run a scan on a local file repository. Using the results of the scan, you determine several documents that are company confidential. You configure a block rule on McAfee DLP Prevent that will trigger if a user tries to send one of these documents in an email message. However, the blocking action must take place on the MTA server. McAfee DLP Monitor will receive copies of all outbound connections initiated by the MTA server. You configure a rule on McAfee DLP Monitor to detect if the MTA server is not properly blocking email messages containing the confidential files.

This illustration shows a simplified network diagram where all McAfee DLP products and ePolicy Orchestrator are deployed.



Reference	Description	Data vector
1	ePolicy Orchestrator connects to McAfee DLP Manager for policy configuration and incident management. McAfee DLP Manager connects to managed McAfee DLP Manager devices for policy and configuration updates.	Not applicable
2	McAfee DLP Endpoint software on endpoint devices monitors and restricts users' data use.	Data in Use
3	McAfee DLP Discover connects to databases and file repositories, scanning data and files to find sensitive information.	Data at Rest
4	McAfee DLP Monitor receives copies of network packets from the LAN switch, either through a SPAN port on the switch or a network tap. McAfee DLP Monitor analyzes and classifies data from network connections.	Data in Motion
5	McAfee DLP Prevent receives email messages from one or more MTA servers. McAfee DLP Prevent analyzes the email messages, adds appropriate headers based on configured policy, and sends the email messages to a single MTA server, also known as the Smart Host.	
6	McAfee DLP Prevent receives web traffic from one or more web proxy servers. McAfee DLP Prevent analyzes the web traffic, determines if the traffic should be allowed or blocked, and sends the traffic back to the appropriate web proxy server.	

Deployment

Chapter 2 *Deployment options*
Chapter 3 *Deployment scenarios*
Chapter 4 *Plan your deployment*

2 Deployment options

The McAfee DLP product suite offers several different options for integration in your network.

Contents

- *Types of installations*
- *Management options*
- *Using McAfee DLP with other McAfee products*

Types of installations

McAfee DLP can be installed on hardware appliances or virtually.

McAfee DLP hardware appliances allow for full performance optimization. These appliance models are supported:

- 5500
- 4400
- 3650
- 1650

Virtual installations allow for multiple instances of McAfee DLP to run on the same system. However, this impacts McAfee DLP performance — service loading time is longer, and network throughput and available disk space is reduced.

Management options

McAfee DLP offers different ways to manage your systems.

Standalone appliances — McAfee DLP Monitor, McAfee DLP Prevent, and McAfee DLP Discover can all operate as standalone appliances. A standalone appliance can be converted to a managed appliance, but policy configuration, captured data, and incidents are lost when converting to a managed appliance.

Choose this option if only one McAfee DLP appliance is deployed on your network.

McAfee DLP Manager — McAfee DLP Manager manages up to 39 McAfee DLP appliances and handles all policy configuration, incident and case management, and reports. This allows you to configure policy, view captured data, and manage incidents from a single user interface. You can create and apply the same rules to multiple McAfee DLP appliances. Incidents generated from managed devices are collected into a central repository for easy correlation of incidents from different devices.

McAfee DLP Manager can integrate with ePolicy Orchestrator to support all management options and configurations, including McAfee DLP Endpoint.

- **McAfee DLP Manager without ePolicy Orchestrator** — Choose this option if multiple McAfee DLP appliances are deployed on your network and you are not using ePolicy Orchestrator.
- **McAfee DLP Manager with ePolicy Orchestrator** — Choose this option if you are managing with ePolicy Orchestrator or integrating the McAfee DLP Endpoint software with McAfee DLP Manager.

If you are using McAfee DLP Endpoint but not any of the McAfee DLP appliance products, McAfee DLP Manager is not required. For more information, see the *McAfee Data Loss Prevention Endpoint Product Guide*.

Using McAfee DLP with other McAfee products

McAfee DLP integrates with several other McAfee products, increasing the functionality of the product suite.

- **ePolicy Orchestrator** — Integrates McAfee DLP Endpoint with McAfee DLP Manager for a unified policy solution

  ePolicy Orchestrator can also be used without McAfee DLP Endpoint to manage McAfee DLP devices
- **McAfee® Logon Collector** — Provides directory credentials for McAfee DLP, extending the amount of user information collected by McAfee DLP
- **McAfee® Email Gateway** — Integrates with McAfee DLP Prevent for email protection
- **McAfee® Web Gateway** — Integrates with McAfee DLP Prevent for web protection

3 Deployment scenarios

Due to the number of McAfee DLP products and the ways to implement them, deployments often differ from network to network.

The following sections discuss different scenarios for initial deployment of McAfee DLP products.

Contents

- *Deployment scenario: McAfee DLP Monitor*
- *Deployment scenario: McAfee DLP Discover and McAfee DLP Prevent*
- *Deployment scenario: Full product suite integration*

Deployment scenario: McAfee DLP Monitor

McAfee DLP Monitor can be installed as a standalone product for initial network assessment.

Use McAfee DLP Monitor to gain an understanding of the types and quantity of data transferred across the network. McAfee DLP Monitor does not block or alter network traffic, which allows it to integrate into a production environment without impacting live traffic.

Example use cases

- McAfee DLP Monitor captures and analyzes the traffic of well-known TCP protocols. If McAfee DLP Monitor cannot classify a connection as a known protocol, it will mark the connection as unknown. Users or devices sending a large volume of unknown traffic might indicate a violation of company policy.
- Some networks require that all internal email messages are sent to a particular email server. McAfee DLP Monitor can detect if users or other devices are bypassing the local email server.
- Some networks require that all web traffic is handled through a proxy server. McAfee DLP Monitor can detect if web traffic is bypassing the proxy server.
- Place a McAfee DLP Monitor appliance on either side of the network border firewall to verify if the firewall allows and blocks the appropriate inbound and outbound connections. Although not required, using McAfee DLP Manager is highly recommended, providing a single console to configure policy and manage incidents from both devices.

Considerations

- McAfee DLP Monitor cannot take any blocking actions on traffic.
- If a standalone McAfee DLP Monitor is added to McAfee DLP Manager at a later time, all policy configurations and incidents will be lost.

High-level steps for implementation

1. Connect the appliance to a switch SPAN port or network tap.
2. Install McAfee DLP Monitor.
3. Enable relevant pre-defined policies and rules.
4. Create additional rules and policies to meet the needs of your network.
5. Review incidents generated by McAfee DLP Monitor.
6. Create capture filters and tune rules as needed to reduce false positives.

Deployment scenario: McAfee DLP Discover and McAfee DLP Prevent

Install McAfee DLP Discover and McAfee DLP Prevent to discover critical documents and prevent these documents from leaving the network in an email message or web upload.

McAfee DLP Discover scans local file repositories and detects highly confidential documents based on the parameters of the scan. McAfee DLP Discover creates high-granularity signatures of these files, allowing McAfee DLP Prevent to detect full or partial document matches within email messages.

Example use case

Configure rules for McAfee DLP Prevent to take different actions on email messages based on the match percentage of the document. If the transmitted document is a 50 to 100 percent match, the email message is blocked, a notification is sent back to the user, and an incident is generated. If the document is a 20 to 49 percent match, the email message is allowed and an incident is generated. If the document match is 19 percent or less, the email message is allowed and an incident is not generated.

This use case similarly applies to a McAfee DLP Prevent appliance configured for web traffic analysis.

Considerations

- Although not required, using McAfee DLP Manager is highly recommended, providing a single console to configure policy and manage incidents.
- Processing both web and email traffic on the same McAfee DLP Prevent appliance is not supported. To implement both web and email protection, you will need to deploy two or more McAfee DLP Prevent appliances.
- McAfee DLP Prevent processes ICAP or SMTP traffic. McAfee DLP Monitor is needed to analyze traffic using other protocols.

High-level steps for implementation

1. Install McAfee DLP Manager and perform initial configuration.
2. Install McAfee DLP Discover and McAfee DLP Prevent.
3. Add McAfee DLP Discover and McAfee DLP Prevent to McAfee DLP Manager using the McAfee DLP Manager interface.
4. Configure and perform scans on file repositories within your network.
5. Register any sensitive documents to McAfee DLP Manager.

6 Configure McAfee DLP Prevent rules to allow or block sensitive documents based on the match percentage.

7 Review incidents reported to the incident dashboards.

Deployment scenario: Full product suite integration

Deploying all McAfee DLP products allows you to take full advantage of all features within the product suite.

In this scenario, McAfee DLP provides protection for all data vectors — Data in Motion, Data at Rest, and Data in Use. All system and policy configurations, incident and case management, and maintenance functions are performed through a single management console provided by ePolicy Orchestrator.

Example use cases

- Identify sensitive data and files with McAfee DLP Discover and configure McAfee DLP Prevent policy to block traffic containing confidential information.
- Scan endpoint devices to identify sensitive files or data, correlating McAfee DLP Endpoint scan results with McAfee DLP Discover scan results.
- Prevent endpoint users from transmitting files to removable media or printers.
- Prevent endpoint users from sending sensitive data in an email message or web upload.
- Configure rules on McAfee DLP Monitor to create incidents for network traffic generated by endpoint devices that do not support McAfee DLP Endpoint.
- Search historical data captured by McAfee DLP Monitor and use the results to adjust McAfee DLP policies to better suit the security needs of your network.
- Group related incidents from multiple McAfee DLP devices into cases, giving you a broader understanding of the nature of the violation.

Considerations

- ePolicy Orchestrator is required.
- Depending on your network environment and security requirements, the number and complexity of policies might increase to utilize the varying functionalities of the different products.

High-level steps for implementation

1 Install and configure ePolicy Orchestrator.

2 Install McAfee DLP Manager and perform initial configuration.

3 Add McAfee DLP Manager to ePolicy Orchestrator.

4 Install any McAfee DLP Monitor, McAfee DLP Prevent, and McAfee DLP Discover appliances.

5 Add managed McAfee DLP devices to McAfee DLP Manager using the ePolicy Orchestrator interface.

6 Install and configure McAfee DLP Endpoint using ePolicy Orchestrator.

7 Enable relevant pre-defined policies and rules.

8 Create additional rules and policies to meet the needs of your network.

9 Review incidents reported to the incident dashboards.

10 Create capture filters and tune rules as needed to reduce false positives.

See also

Integrating multiple McAfee DLP products on page 20

4 Plan your deployment

Prepare your appliance for installation and integration into the network.

Contents

- *Product-specific requirements*
- *Network placement*
- *Default ports used in McAfee DLP communications*
- *Order of deployment*
- *Deployment Checklist*

Product-specific requirements

McAfee DLP Monitor, McAfee DLP Prevent, and McAfee DLP Discover have specific requirements for network integration.

Network integration requirements for McAfee DLP Monitor

McAfee DLP Monitor requires the use of a switch SPAN port or network tap for network integration.

When determining which method to implement, take these points into consideration.

Table 4-1 Integration considerations

Method	Is network downtime required?	Are all packets captured?
SPAN port	No	No — Under heavy loads, packets might be dropped.
Network tap	Yes — Cables from neighboring devices must be disconnected and connected to the tap.	Yes

If both capture ports on McAfee DLP Monitor are used, make sure the traffic on the ports is different, such as different subnets. McAfee DLP Monitor should not receive the same connections on both ports.

Integration using a switch SPAN port

When using a SPAN port, packets from the switch are copied, or mirrored, to the McAfee DLP Monitor appliance.

Certain switch models permit the use of the remote SPAN (RSPAN) capability, which allows ports from multiple switches to mirror traffic to the McAfee DLP Monitor appliance. If you want to mirror multiple ports on multiple switches to your McAfee DLP Monitor appliance, contact the switch vendor for details on configuring RSPAN.

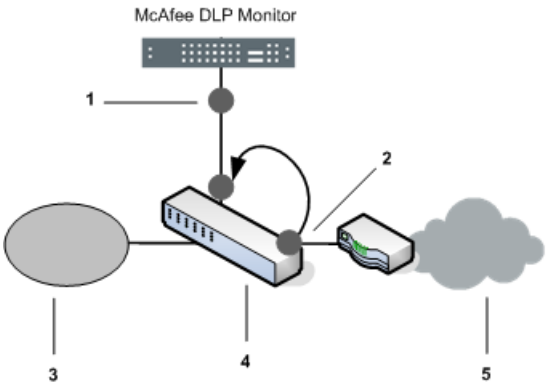


Figure 4-1 Span port configuration

1	Capture ports
2	WAN router traffic mirrored to McAfee DLP Monitor port
3	LAN
4	LAN switch
5	WAN

Integration using a network tap

A network tap is attached to the LAN switch and WAN router through two network ports and captures all traffic. Traffic from these ports flows directly to the capture ports on McAfee DLP Monitor.

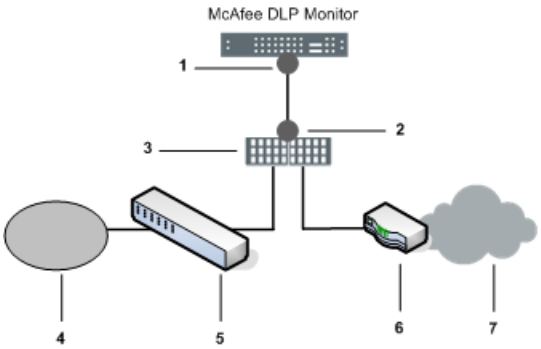


Figure 4-2 Network tap configuration

1 Capture ports	5 LAN switch
2 Analyzer ports	6 Router
3 Network tap	7 WAN
4 LAN	

Requirements for configuring MTA servers with McAfee DLP Prevent

Your MTA server must meet several requirements in order to integrate with McAfee DLP Prevent.

- The MTA server sends all or a portion of email traffic to McAfee DLP Prevent.

  Example: In some environments, it might be preferable for McAfee DLP Prevent to process only mail going to or from public sites, such as Gmail, rather than processing every email sent and received on the network.

- The MTA server inspects email headers.
- The MTA server distinguishes email arriving from McAfee DLP Prevent and acts on header strings in email messages — specifically, X-RCIS-Action headers with values ALLOW, BLOCK, QUART, ENCRYPT, BOUNCE, REDIR and NOTIFY.

  If certain actions are not supported on the MTA server, do not configure rules on McAfee DLP Prevent to use these actions.

- All email messages the MTA server receives from McAfee DLP Prevent are routed to the proper destination, and not back to McAfee DLP Prevent.

  Example: Routing might be defined using a port number or source IP address, or by checking if X-RCIS-Action headers are present.

- McAfee DLP Prevent supports up to 30 concurrent SMTP connections. If supported by the MTA server, McAfee recommends configuring the MTA server to limit the number of connections to McAfee DLP Prevent to 25.

Supported repositories with McAfee DLP Discover

McAfee DLP Discover supports several common database repositories, file systems, and servers.

Table 4-2 Supported repositories

Database repositories	File systems and servers

• DB2 — 5x iSeries, 6.1 iSeries, 7.x–9.x
• Microsoft SQL Server 2000, 2005, 2008, 7.0, MSDE 2000
• MySQL (Enterprise) 5.0.x, 5.1
• Oracle 8i, 9i, 10g, 11g
	• EMC Celerra 5.6
	• EMC Documentum 5.3, 6.0, 6.5
	• Microsoft SharePoint 2007, 2010
	• FTP
	• HTTP/HTTPS
	• NFS (Network File System)
	• CIFS (Common Internet File System)
	  • Microsoft Windows Server 2003, 2008, 2008 R2 cluster
	  • Microsoft Windows XP Professional SP3 or later (32-bit)
	  • Microsoft Windows Vista SP1 or later Enterprise and Business editions (32-bit)
	  • Microsoft Windows 7 SP1 or later (32- and 64-bit)
	  • NetApp 7.2, 7.3

Network placement

Consider these points before adding McAfee DLP appliances to your network.

- McAfee DLP Manager must be on the same LAN as managed devices. For deployments involving separate networks, such as different physical locations, install additional McAfee DLP Manager appliances for managing local devices.
- McAfee DLP devices must be able to communicate with other appropriate devices for successful deployment and functionality. Any intermediate routers, firewalls, or policy-enforcing devices must be configured to accommodate traffic between devices.
- The placement of McAfee DLP Monitor determines what data is captured. Although McAfee DLP Monitor can connect to any switch in your network by means of a SPAN port or network tap, McAfee DLP Monitor typically connects to the LAN switch before the WAN router. This placement ensures that all connections entering or leaving the network are captured by McAfee DLP Monitor.
- Large amounts of SMTP or ICAP connections can be split between multiple McAfee DLP Prevent appliances by using load-balancing devices. Verify the configuration on the load-balancing devices to ensure there is no overlap between the connections received by the McAfee DLP Prevent appliances.

Default ports used in McAfee DLP communications

McAfee DLP appliances use many ports for various network connections. Configure any intermediary firewalls or policy-enforcing devices to allow these ports where necessary.

All listed protocols use TCP only, unless noted otherwise.

Table 4-3 Default ports used in management and general network communications

Source	Destination	Destination port	Protocol	Details
Any	Any McAfee DLP appliance	22	SSH	Administrators connect to the command line interface for installations, upgrades, and other administrative activities.
		161	SNMP (UDP)	External SNMP monitoring applications connect to the McAfee DLP appliance to query hardware and system status.
		443	HTTPS	Administrators connect to the web-based user interface to configure McAfee DLP and view incident data. For managed appliances, the McAfee DLP Manager web interface is used. The web interface on managed devices allows read-only operations.
Any McAfee DLP appliance	Corporate email server	25	SMTP	McAfee DLP appliances send email notifications when certain events are triggered.
	NTP server	123	NTP (UDP)	McAfee DLP connects to an NTP server for time synchronization.

Table 4-3 Default ports used in management and general network communications *(continued)*

Source	Destination	Destination port	Protocol	Details
	Syslog server	154	Syslog (UDP)	McAfee DLP appliances send syslog notifications when certain events are triggered.
	SNMP trap server	162	SNMPTrap (UDP)	McAfee DLP appliances send SNMP trap notifications regarding hardware and system events.
McAfee DLP Manager	Any McAfee DLP appliance	22	SSH	McAfee DLP Manager connects to managed devices for configuration and data transfer.
		49158	TCP	McAfee DLP Manager connects to managed appliances for system process communication.
	ePolicy Orchestrator server	1433	TCP	McAfee DLP Manager copies Data in Use events from the ePolicy Orchestrator database.
	LDAP or Active Directory server	• 389 (Non-SSL) • 636 (SSL)	LDAP	McAfee DLP Manager connects to authentication servers for user details.
	McAfee Logon Collector	61641	TCP	McAfee DLP Manager connects to McAfee Logon Collector for user details.
ePolicy Orchestrator server	McAfee DLP Manager	443	HTTPS	ePolicy Orchestrator connects to McAfee DLP Manager to display the user interface.
		3306	TCP	ePolicy Orchestrator copies incidents from the McAfee DLP Manager database.

Table 4-4 Default ports used in McAfee DLP Discover communications

Source	Destination	Destination port	Protocol	Details
McAfee DLP Discover	CIFS repository	139	NetBIOS	McAfee DLP Discover connects to the server or repository for a file or database scan.
		445	SMB	
	DB2 server	50000	TCP	
	EMC Documentum server	1489	TCP	
	FTP server	• 20 • 21	FTP	
	HTTP server	80	HTTP	
	HTTPS server	443	HTTPS	
	MS SQL server	1433	TCP	
	MySQL server	3306	TCP	

Table 4-4 Default ports used in McAfee DLP Discover communications *(continued)*

Source	Destination	Destination port	Protocol	Details
	NFS repository	• 111 • 2049	NFS	
	Oracle server	1521	TCP	
	SharePoint server	80	HTTP	
		443	HTTPS	

Table 4-5 Default ports used in McAfee DLP Prevent communications

Source	Destination	Destination port	Protocol	Details
McAfee DLP Prevent	MTA server	25	SMTP	McAfee DLP Prevent connects to the MTA server for delivering processed emails.
	Web proxy server	1344	ICAP	McAfee DLP Prevent connects to the web proxy server for delivering processed web traffic.
MTA server	McAfee DLP Prevent	25	SMTP	The MTA server connects to McAfee DLP Prevent for delivering email messages for analysis.
Web proxy server	McAfee DLP Prevent	1344	ICAP	The web proxy server connects to McAfee DLP Prevent for delivering web traffic for analysis.

Order of deployment

When integrating multiple McAfee DLP products, consider these points.

- If you are using McAfee DLP Manager, install McAfee DLP Manager first, then install the appliances that are to be managed. After installation, add the managed appliances to McAfee DLP Manager. If you perform any configurations on standalone devices, those configurations are lost after adding the device to McAfee DLP Manager.
- If you are using both McAfee DLP Monitor and McAfee DLP Prevent on the same network, consider installing McAfee DLP Monitor first.

  Example: If this is your first time using McAfee DLP on your network, gain a general understanding of what types of data are sent across your network before implementing a McAfee DLP Prevent policy that blocks live network connections.
- If you are using ePolicy Orchestrator for McAfee DLP management, McAfee recommends installing the products in this order:

  1 Install and configure ePolicy Orchestrator.

  2 Install McAfee DLP Manager and perform initial configuration.

  3 Add McAfee DLP Manager to ePolicy Orchestrator.

4 Install any McAfee DLP Monitor, McAfee DLP Prevent, and McAfee DLP Discover appliances.

5 Add managed McAfee DLP devices to McAfee DLP Manager using the ePolicy Orchestrator interface.

Deployment Checklist

Before installing McAfee DLP products, verify that you have the necessary information for a successful deployment.

- Determine if your installations will be virtual, on hardware appliances, or a combination of both. Virtual appliances can run on your own VMware ESX or ESXi server, or you can install an ESX or ESXi server on McAfee DLP hardware.
- If you are installing multiple McAfee DLP products, determine your management method. If you are integrating McAfee DLP Endpoint with other McAfee DLP products, ePolicy Orchestrator is required.
- If you are using McAfee DLP Monitor, determine if you will be using a switch SPAN port or a network tap for integration.
- If you are using McAfee DLP Prevent for both web and email protection, you will need at least two McAfee DLP Prevent installations. A single McAfee DLP Prevent appliance does not support web protection and email protection at the same time.
- Verify that any ports needed for McAfee DLP communications are opened on any firewalls or policy-enforcing devices.
- Gather basic network information for your McAfee DLP appliances.
  - Host name
  - IP address
  - Subnet mask
  - Default gateway
  - DNS domain
  - Primary DNS server
  - Secondary DNS server
  - Active Directory Server
  - NTP server
  - Syslog server
  - Email relay server
  - SNMP trap server

Installation

Chapter 5 *Set up the hardware*
Chapter 6 *Install or upgrade the system*
Chapter 7 *Complete post-installation tasks*

5 Set up the hardware

Prepare the hardware for installation and integration in the network.

Contents

- *Check the shipment*
- *Rack mount the appliance*
- *Identify network ports*
- *Configure SPAN or tap mode for McAfee DLP Monitor*
- *Connect the management port*

Check the shipment

Each product ships with all the items needed to install the appliance on a network. Check the content list included with the shipment to verify that you received all the necessary items.

If an item is missing or damaged, contact your supplier.

Rack mount the appliance

Install the appliance in a server rack.

For additional information on rack mounting appliances, visit:

http://download.intel.com/support/motherboards/server/sr870bh2/sb/sr870bh2railkitinstallinstructions0503.pdf

Identify network ports

McAfee DLP appliances have one management port and two capture ports.

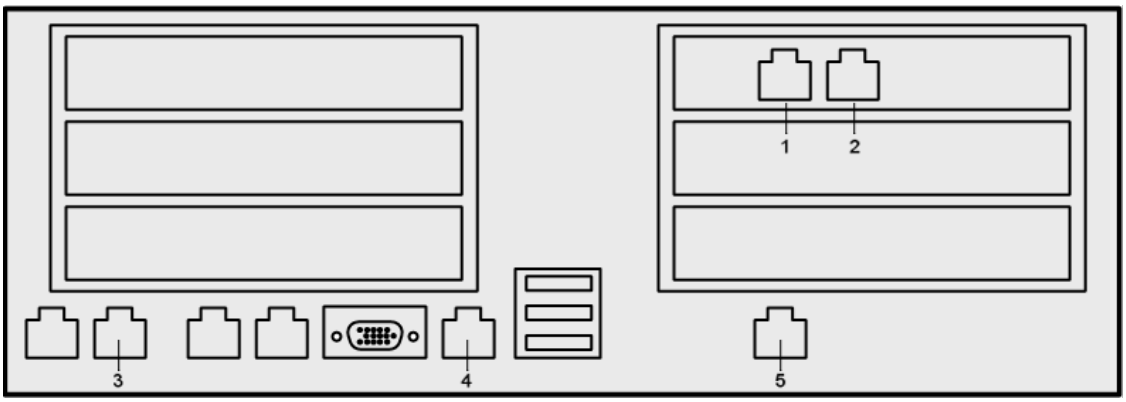


Figure 5-1 Model 5500 appliance port configuration

1 Capture port 1 (Ethernet port 3)	**4** Serial port
2 Capture port 0 (Ethernet port 2)	**5** Remote access port
3 Management port (Ethernet port 1)	

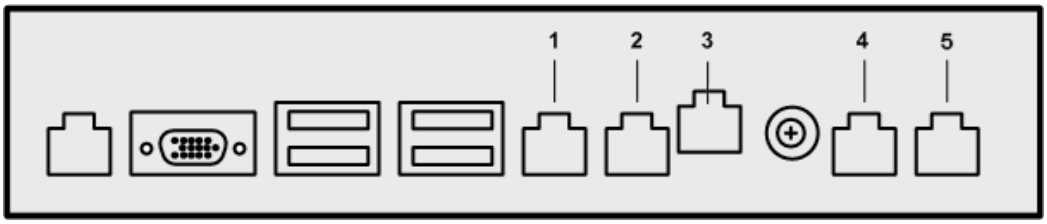


Figure 5-2 Model 4400 appliance port configuration

1 Unused (Ethernet port 0)	**4** Capture port 1 (Ethernet port 2)
2 Management port (Ethernet port 1)	**5** Capture port 0 (Ethernet port 3)
3 Remote access port	

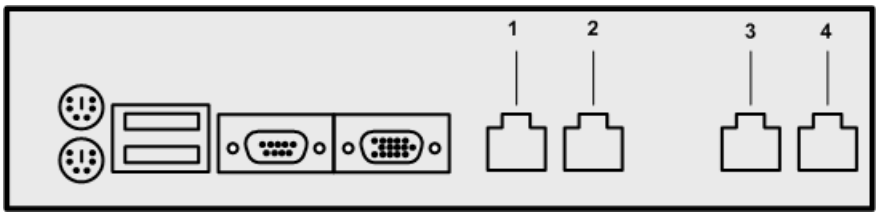


Figure 5-3 Model 1650 appliance port configuration

1	Unused
2	Management port (Ethernet port 1)
3	Capture port 0 (Ethernet port 2)
4	Capture port 1 (Ethernet port 3)

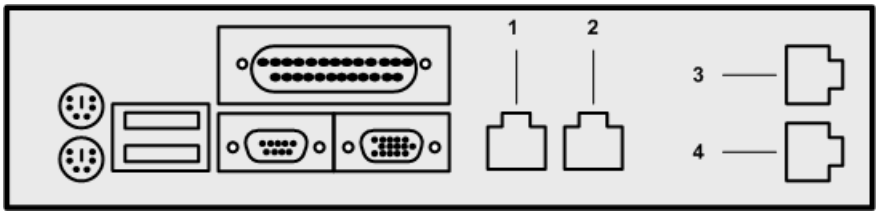


Figure 5-4 Model 3650 appliance port configuration

1	Unused
2	Management port (Ethernet port 1)
3	Capture port 0 (Ethernet port 2)
4	Capture port 1 (Ethernet port 3)

Configure SPAN or tap mode for McAfee DLP Monitor

Integrate McAfee DLP Monitor into your network using the method best suited to your network.

See also

Network integration requirements for McAfee DLP Monitor on page 31

Integrate the appliance using a SPAN port

Connect the appliance to the network using a SPAN configuration.

Task

1. Connect the McAfee DLP Monitor capture port to the switch SPAN port.
2. Log on to the switch and apply the appropriate SPAN port configuration. For information on configuring the switch, see the vendor documentation for your switch.
3. On the switch, use interface commands, such as `show`, to verify that the switch port connected to McAfee DLP Monitor is receiving traffic.
4. Save the configuration on the switch.

Integrate the appliance using a network tap

Connect the appliance to the network using a network tap configuration.

Task

1. Disconnect the cable between your WAN router and your LAN switch.
2. Connect the network tap to the WAN router, the LAN switch, and the McAfee DLP Monitor capture port. For information on cabling the network tap, see the vendor documentation for your network tap.

Connect the management port

Connecting a computer, such as a laptop, to the McAfee DLP appliance allows you to configure the appliance IP address and other parameters for integration in the network.

By default, each appliance is configured with the IP address 192.168.1.2.

Task

1. Connect a computer to the management port of the appliance using the supplied Ethernet cable.
2. Configure the computer to use an IP address in the 192.168.1.0/24 range, such as 192.168.1.10.

See also

Identify network ports on page 42

6 Install or upgrade the system

All appliances are shipped with McAfee DLP Manager pre-installed.

Any McAfee DLP appliance can be converted to a different McAfee DLP product by performing a full installation.

Only one product can be installed on the appliance at a time. On model 4400 and 5500 appliances, the primary and secondary images must both be installed with the same product.

For information on performing a virtual installation of McAfee DLP, see the *McAfee Data Loss Prevention Virtual Appliance Installation Guide*.

Contents

- *Installing or upgrading the software on 4400 and 5500 appliances*
- *Installing or upgrading the software on 1650 and 3650 appliances*
- *Applying hotfixes*
- *Re-imaging an appliance*

Installing or upgrading the software on 4400 and 5500 appliances

4400 and 5500 appliances contain two images, each containing an operating system and McAfee DLP software.

Primary and secondary images are initially duplicate installations. When the system is upgraded, the two images can contain different versions of the same product. The system automatically boots from the latest installed version by default.

Download the 4400 or 5500 archive

Download the software from the McAfee downloads site.

Before you begin

Locate the grant number you received after purchasing the product.

Table 6-1 Product archive names

Product	Archive name
McAfee DLP Manager	imanager
McAfee DLP Monitor	iguard
McAfee DLP Prevent	iprevent
McAfee DLP Discover	idiscover

Task

1 In a web browser, go to www.mcafee.com/us/downloads/downloads.aspx.

2 Enter your grant number, then select the appropriate product and version.

3 In the **Software Downloads** tab, select and save the appropriate *.tgz file.

Install a new image on 4400 or 5500 appliances

Install a new image on the primary and secondary disks.

Before you begin

Download the product archive and copy it to the appliance.

Task

1 Using a command line session, log on to the appliance as root.

The default root password is *mcafee*.

2 Make an installation directory.

```
# mkdir /data/install
```

3 Copy the archive to the appliance.

- If you downloaded the archive to a Windows-based computer, use WinSCP.
- If you downloaded the archive to a Linux server, log on to the server and use the SCP command.

```
scp -rp <filename> root@<name or ip address>:/data/install
```

4 Go to the /data/install directory.

```
# cd /data/install
```

5 Extract the contents of the archive.

```
# tar xvzf ndlp_<product>.tgz
```

6 Run the installation script.

Before you type in the command, run `pwd` to establish that you are in the correct product directory. You must be sure that you are running the updated scripts in the upgrade archive that you just downloaded and extracted.

```
# ./install_new_full <product> .
```

where `<product>` is *imanager*, *iguard*, *idiscover* or *iprevent*.

The product image installs on the primary and secondary disks.

7 Restart the system.

```
# reboot
```

Restarting the system might take 10–15 minutes.

8 Log on to the appliance as root and verify the installation.

If you are using the default root password, you are prompted to change the password after logging on.

```
# cat /data/stingray/etc/version
```

If the **Release** field contains 9.3.0, installation is complete.

If the installation fails, do not perform the installation again. Call McAfee support and submit an installation log file.

Upgrading appliances in a managed environment

Upgrading McAfee DLP products that are managed by McAfee DLP Manager requires additional planning.

McAfee recommends performing these high-level steps when upgrading managed McAfee DLP products.

1 Stop all scans and search tasks on the McAfee DLP Manager, and wait until they are completely stopped.

2 Perform a backup on McAfee DLP Manager.

3 Upgrade McAfee DLP Manager to version 9.3.0.

4 Upgrade managed McAfee DLP Monitor, McAfee DLP Prevent, and McAfee DLP Discover appliances to version 9.3.0.

Consider these points when upgrading in a managed environment:

- After upgrading McAfee DLP Manager to version 9.3.0, McAfee DLP Manager cannot connect to managed appliances running versions 9.2.0, 9.2.1, or 9.2.2. Managed appliances continue to enforce the current McAfee DLP policies and collect incidents and captured data locally.
- McAfee does not recommend you change the configuration on an upgraded McAfee DLP Manager until all managed appliances are also upgraded. During this time, you can view incidents collected before the upgrade, but opening evidence files or trying to create a case might fail.
- After upgrading a managed appliance to version 9.3.0, the appliance automatically reconnects to McAfee DLP Manager. McAfee DLP Manager receives copies of incidents accumulated on the managed appliances during the time the appliances were disconnected.

Upgrade the products on 4400 or 5500 appliances

If your product is at version 9.2.0, 9.2.1, or 9.2.2, you can upgrade directly to 9.3.0.

Before you begin

- Download the product archive.
- Stop all scans and search tasks, and wait until they are completely stopped.

- If you are running version 9.2.0 on a McAfee DLP Manager or a standalone McAfee DLP product on a model 4400 appliance, and you want to perform a backup before upgrading, you must apply hotfix 754037_45668_01.

McAfee recommends performing frequent backups. Without a backup, the data, settings, and configuration on your appliance might be lost in the event of a system failure.

- To upgrade a product, you must install the new image on the disk that is *not* used by the previous installation. This ensures that the original image can still be accessed after the upgrade is complete. The system automatically boots from the latest image.

  The `install_to_pri` and `install_to_sec` scripts install the upgrade. After the process runs, the existing configuration and database are copied to the new image.

  If you use the wrong script, you will write over your existing installation.

Task

1. Using a command line session, log on to the appliance as root.
2. Make an installation directory.

   ```
   # mkdir /data/install
   ```

3. Copy the archive to the appliance.
   - If you downloaded the archive to a Windows-based computer, use WinSCP.
   - If you downloaded the archive to a Linux server, log on to the server and use the SCP command.

     ```
     scp -rp <filename> root@<name or ip address>:/data/install
     ```

4. Verify which version is currently installed. You must be at version 9.2.0, 9.2.1, or 9.2.2 to upgrade to version 9.3.0.

   ```
   # cat /data/stingray/etc/version
   ```

5. Go to the /data/install directory.

   ```
   # cd /data/install
   ```

6. Extract the contents of the archive.

   ```
   # tar xvzf ndlp_<product>.tgz
   ```

7. Run the `system_info` utility to determine if the system is currently using the primary or secondary image.

   ```
   # /data/stingray/ksh/system_info
   ```

   Install the update on the disk that is *not* used.

   Example: Install the update on the **secondary** disk with `install_to_sec` if `system_info` returns this message:

   "The system is currently running <product> from the **primary** image."

8. Run the installation script.

   Before you type the command, run `pwd` to establish that you are in the correct product directory. You must be sure that you are running the updated scripts in the upgrade archive that you just downloaded and extracted.

   ```
   # ./install_to_pri <product> .
   ```

   or

   ```
   # ./install_to_sec <product> .
   ```

   where `<product>` is *imanager*, *iguard*, *idiscover* or *iprevent*.

   The product image installs on the primary or secondary disk. When the upgrade is complete, a message appears stating which image the appliance will boot to next.

9 Restart the system.

```
# reboot
```

Restarting the system might take 10–15 minutes.

10 Log on to the appliance as root and verify the installation.

If you are using the default root password, you are prompted to change the password after logging on.

```
# cat /data/stingray/etc/version
```

If the **Release** field contains 9.3.0, installation is complete.

If the installation fails, do not perform the installation again. Call McAfee support and submit an installation log file.

Boot options

Model 4400 and 5500 appliances contain a boot loader package, allowing you to switch between installations.

McAfee DLP uses GNU GRUB (GRand Unified Bootloader) to install the primary and secondary images.

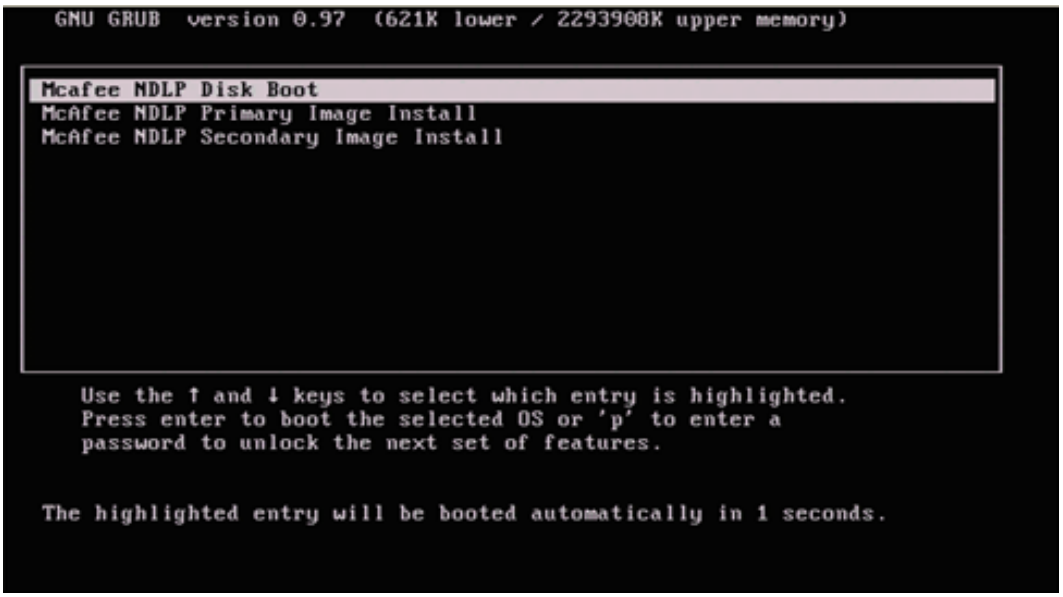

GNU GRUB version 0.97 (621K lower / 2293908K upper memory)
Mcafee NDLP Disk Boot
McAfee NDLP Primary Image Install
McAfee NDLP Secondary Image Install
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS or 'p' to enter a
password to unlock the next set of features.
The highlighted entry will be booted automatically in 1 seconds.

Figure 6-1 McAfee DLP GRUB boot menu

The default **Disk Boot** option is only used to boot the operating system of the appliance.

During the upgrade process, the configuration data in the /data directory and the kernel/boot loader information in the boot directory are copied over to the new installation.

Table 6-2 Boot options

Option	Definition
McAfee NDLP Disk Boot	The system is restarted from the operating system disk. This does not re-install the operating system or the product software.
McAfee NDLP Primary Image Install	The primary image is loaded to the system. This replaces the existing operating system and product software, but retains the data in the /data and /boot directories.
McAfee NDLP Secondary Image Install	The secondary image is loaded to the system. This replaces the existing operating system and product software, but retains the data in the /data and /boot directories.

Set the next boot image

After you install an image, the system automatically assigns the next boot to the image that was installed.

In rare instances, you might want to override this assignment. If you recently performed an upgrade, but you need to revert back to the pervious version, configure the next boot to a different image.

Using this command has the same effect as changing the boot option using the GRUB menu.

Task

1 Using a command line session, log on to the appliance as root.

2 Run the `setnextboot` script to select one of three boot options: primary, secondary, or boot from the operating system on the appliance.

```
# setnextboot [reboot_only | pri | sec]
```

The script sets the selected option. When the option is set, a message appears stating which image will boot next.

3 Restart the system.

```
# reboot
```

Installing or upgrading the software on 1650 and 3650 appliances

Software on 1650 and 3650 appliances is upgraded by running two scripts — one to install operating system components, and another to install the McAfee DLP application.

Download the 1650 or 3650 archive

Download the software from the McAfee downloads site.

Before you begin

Locate the grant number you received after purchasing the product.

Table 6-3 Product archive names

Product	Archive name
McAfee DLP Manager	imanager
McAfee DLP Monitor	iguard

Table 6-3 Product archive names *(continued)*

Product	Archive name
McAfee DLP Prevent	iprevent
McAfee DLP Discover	idiscover

Task

1 In a web browser, go to www.mcafee.com/us/downloads/downloads.aspx.

2 Enter your grant number, then select the appropriate product and version.

3 In the **Software Downloads** tab, select and save the appropriate *.bz2 file.

Install a new image on 1650 or 3650 appliances

To install a product on 1650 or 3650 appliances, run the platform and application scripts.

Before you begin

Download the product archive and copy it to the appliance.

Task

1 Using a command line session, log on to the appliance as root.

2 Make an installation directory.

```
# mkdir /data/install
```

3 Copy the archive to the appliance.

- If you downloaded the archive to a Windows-based computer, use WinSCP.
- If you downloaded the archive to a Linux server, log on to the server and use the SCP command.

```
scp -rp <filename> root@<name or ip address>:/data/install
```

4 Go to the /data/install directory.

```
# cd /data/install
```

5 Extract the contents of the archive.

```
# tar jxf <product>.bz2
```

6 Run the platform installation script.

Enter `./install_platform` for help on available options.

```
# ./install_platform -P <platform type>
```

After the platform script finishes, you might be instructed to restart the system. This message can be ignored; you do not need to restart the system until after the Stingray script finishes.

7 Run the application installation script.

```
# ./install_stingray -P <platform type>
```

The script finishes, then instructs you to restart.

8 Restart the system.

```
# reboot
```

Restarting the system might take 10–15 minutes.

9 Log on to the appliance as root and verify the installation.

If you are using the default root password, you are prompted to change the password after logging on.

```
# cat /data/stingray/etc/version
```

If the **Release** field contains 9.3.0, installation is complete.

If the installation fails, do not perform the installation again. Call McAfee support and submit an installation log file.

Upgrading appliances in a managed environment

Upgrading McAfee DLP products that are managed by McAfee DLP Manager requires additional planning.

McAfee recommends performing these high-level steps when upgrading managed McAfee DLP products.

1 Stop all scans and search tasks on the McAfee DLP Manager, and wait until they are completely stopped.

2 Perform a backup on McAfee DLP Manager.

3 Upgrade McAfee DLP Manager to version 9.3.0.

4 Upgrade managed McAfee DLP Monitor, McAfee DLP Prevent, and McAfee DLP Discover appliances to version 9.3.0.

Consider these points when upgrading in a managed environment:

- After upgrading McAfee DLP Manager to version 9.3.0, McAfee DLP Manager cannot connect to managed appliances running versions 9.2.0, 9.2.1, or 9.2.2. Managed appliances continue to enforce the current McAfee DLP policies and collect incidents and captured data locally.
- McAfee does not recommend you change the configuration on an upgraded McAfee DLP Manager until all managed appliances are also upgraded. During this time, you can view incidents collected before the upgrade, but opening evidence files or trying to create a case might fail.
- After upgrading a managed appliance to version 9.3.0, the appliance automatically reconnects to McAfee DLP Manager. McAfee DLP Manager receives copies of incidents accumulated on the managed appliances during the time the appliances were disconnected.

Upgrade the products on 1650 or 3650 appliances

If your product is at version 9.2.0, 9.2.1, or 9.2.2, you can upgrade directly to 9.3.0.

Before you begin

- Download the product archive and copy it to the appliance.
- Stop all scans and search tasks, and wait until they are completely stopped.

McAfee recommends performing a backup before upgrading. Without a backup, the data, settings, and configuration on your appliance might be lost in the event of a system failure.

Task

1 Using a command line session, log on to the appliance as root.

2 Make an installation directory.

```
# mkdir /data/install
```

3 Copy the archive to the appliance.

- If you downloaded the archive to a Windows-based computer, use WinSCP.
- If you downloaded the archive to a Linux server, log on to the server and use the SCP command.

```
scp -rp <filename> root@<name or ip address>:/data/install
```

4 Verify which version is currently installed. You must be at version 9.2.0, 9.2.1, or 9.2.2 to upgrade to version 9.3.0.

```
# cat /data/stingray/etc/version
```

5 Go to the /data/install directory.

```
# cd /data/install
```

6 Extract the contents of the archive.

```
# tar jxf <product>.bz2
```

7 Run the platform installation script.

Type `./install_platform` for help on available options.

```
# ./install_platform -U -P <platform type>
```

After the platform script finishes, you might be instructed to restart the system. This message can be ignored; you do not need to restart the system until after the Stingray script finishes.

8 Run the application installation script.

```
# ./install_stingray -U -P <platform type>
```

The script completes, then instructs you to reboot.

9 Restart the system.

```
# reboot
```

Restarting the system might take 10–15 minutes.

10 Log on to the appliance as root and verify the installation.

If you are using the default root password, you are prompted to change the password after logging on.

```
# cat /data/stingray/etc/version
```

If the **Release** field contains 9.3.0, installation is complete.

If the installation fails, do not perform the installation again. Call McAfee support and submit an installation log file.

Applying hotfixes

Hotfixes for McAfee DLP products are occasionally released, which address issues found in the product.

Hotfixes are available on the McAfee downloads site, along with the installation archive files. For information on a hotifx, including installation instructions and what issue the hotfix addresses, see the release notes for that hotfix.

Re-imaging an appliance

To re-image an appliance and restore the drives to their pre-installed state, see the *McAfee Data Loss Prevention Hardware Guide*.

7 Complete post-installation tasks

After installation is successful, perform initial configurations on your McAfee DLP devices.

Contents

- *Configure McAfee DLP Manager*
- *Add McAfee DLP Manager to ePolicy Orchestrator*
- *Add McAfee DLP devices to McAfee DLP Manager*
- *Configure standalone McAfee DLP appliances using the Setup Wizard*
- *Configure servers for McAfee DLP Prevent*
- *Link negotiation for McAfee DLP appliances*
- *Testing the system*
- *Additional tasks*

Configure McAfee DLP Manager

Perform the initial configuration on McAfee DLP Manager.

Task

1 Open a web browser and connect to the McAfee DLP appliance.

- For an upgrade or re-installation, enter the appliance's configured IP address.
- For a completely new installation, use the computer connected to the management port and enter:

  `https://192.168.1.2`

2 Log on to the user interface.

The default credentials are `admin`/`mcafee`. After logging on, you are required to change the default password and log on with the new credentials. If you are using the default root password, you must log on to the command line interface to change the root password.

3 On the **End User License Agreement** page, select the checkbox and click **I Accept**.

4 Select **System** | **System Administration** | **Devices**.

5 Click **Configure**.

6 Change parameters on the **System Configuration** page.

7 Click **Update** after each change is made.

Add McAfee DLP Manager to ePolicy Orchestrator

If ePolicy Orchestrator will be used to manage McAfee DLP devices, integrate McAfee DLP Manager with ePolicy Orchestrator.

Install the network extension

Download and install the network extension to ePolicy Orchestrator.

Before you begin

Locate the grant number you received after purchasing the product.

Task

1. In a web browser, go to www.mcafee.com/us/downloads/downloads.aspx.
2. Enter your grant number, then select the appropriate product and version.
3. Download the network extension file, netdlp.zip.
4. In ePolicy Orchestrator, select **Menu** | **Software** | **Extensions**.
5. Click **Install Extension**.
6. Browse to the netdlp.zip file and click **OK**.
7. Click **OK**.

Add an ePolicy Orchestrator database user

Database access is needed to transfer events and policy updates between ePolicy Orchestrator and McAfee DLP Manager.

The database user name is *espouser* and cannot be changed.

Task

1. On your McAfee DLP appliance, select **System** | **User Administration** | **DB User**.
2. On the **ePO User Information** page, enter and confirm a password.
3. In the **IP Address** field, enter an IP address for the ePolicy Orchestrator database, then click **Add** to add it to the **Selected IP Addresses** list.

   Repeat if there are additional ePolicy Orchestrator databases.
4. Click **Apply**.

Register McAfee DLP Manager on ePolicy Orchestrator

Use the ePolicy Orchestrator interface to add McAfee DLP Manager as a registered server.

Task

1. In ePolicy Orchestrator, select **Menu** | **Configuration** | **Registered Servers**.
2. Click **New Server**.
3. Type the name of the McAfee DLP Manager, add optional notes, and click **Next**.

   The **Registered Server Builder** page appears.
4. In the **Description** field, type in the name of the McAfee DLP Manager.

5 In the **Database Password** field, enter the *epouser* database password from the McAfee DLP Manager **System** | **User Administration** | **DB User** page.

6 If there is existing data on McAfee DLP Manager, select the **Copy Incidents/Device Data**.

7 Enter the user name and password to McAfee DLP Manager and set the refresh period.

8 Click **Test Connection**.

9 If the test is successful, click **OK**.

Install the host extension

Download and install the host extension to ePolicy Orchestrator.

Before you begin

Locate the grant number you received after purchasing the product.

If you already have McAfee DLP Endpoint installed and configured on ePolicy Orchestrator, do not re-install this extension.

Task

1 In a web browser, go to www.mcafee.com/us/downloads/downloads.aspx.

2 Enter your grant number, then go to the appropriate product and version.

3 Download the host extension file, HDLP_Extension_x_x_x_xxx.zip.

4 In ePolicy Orchestrator, select **Menu** | **Software** | **Extensions**.

5 Click **Install Extension**.

6 Browse to the host extension on your desktop and click **OK**.

7 Click **Policy Catalog** and select **View/Duplicate** to configure the agent.

The McAfee DLP Endpoint Management Tools installer runs, then the agent configuration console begins loading. Add the required information to the fields.

8 Assign this policy to the agent.

If you intend to use McAfee DLP Endpoint, the protection rules will not work unless the agent is deployed to endpoint devices.

Required ePolicy Orchestrator registration information

Information about the ePolicy Orchestrator server, database and user interface is needed when registering to McAfee DLP Manager.

Most of the required information can be found in the ePolicy Orchestrator user interface. Log on to the ePolicy Orchestrator server using this URL:

```
https://<server name or IP address>:<port>/core/config
```

Table 7-1 Sources for ePolicy Orchestrator data

McAfee DLP Manager user interface option	Where to find data
EPO Database IP address or hostname	**Menu** | **Configuration** | **Registered Servers** (local ePolicy Orchestrator server)
EPO Database password	The SQL password created in **Microsoft SQL Server Management Studio**
EPO Database port	**SQL Server Configuration Manager** | **TCP/IP Properties** | **IP Addresses** | **TCP Ports**
EPO Database user	The user name created in **Microsoft SQL Server Management Studio**
EPO Database	**Menu** | **Configuration** | **Registered Servers** | **Actions** | **Edit** | **Next** | **Database instance**
EPO Database instance	**Menu** | **Configuration** | **Registered Servers** | **Actions** | **Edit** | **Next** | **SQL Server instance** | **instance name**
EPO GUI IP address	Address bar of ePolicy Orchestrator server
EPO GUI user	User account name used to log on to ePolicy Orchestrator server
EPO GUI password	User account password used to log on to ePolicy Orchestrator server
EPO GUI port	Address bar of ePolicy Orchestrator server

Register ePolicy Orchestrator on McAfee DLP Manager

Use the McAfee DLP Manager interface to add ePolicy Orchestrator as a device.

Task

1 On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 Select **Actions** | **New Device**.

3 Select **Check here to add an EPO device**.

4 Enter the requested information.

If **Incident Copy Only** is selected, ePolicy Orchestrator will not route policy updates to endpoint devices.

5 Click **Add**.

6 Click **OK** to confirm the registration.

7 To check the status, refresh the page.

When the **Status** icon in the device list to turns green, registration is complete.

Add McAfee DLP devices to McAfee DLP Manager

Adding a device to McAfee DLP Manager will remove the current policy, configuration, incidents, and cases on the device.

Before you begin

If you are using the default root password on a McAfee DLP device, log on to the command line interface of the McAfee DLP device to change the password before adding the device to McAfee DLP Manager.

If there is any existing configuration or data on the device, McAfee recommends reinstalling the appliance before adding it to McAfee DLP Manager.

Devices added to McAfee DLP Manager will be assigned any policies that are configured for **All Devices**. If **All Devices** is not selected in a policy, the policy must be manually configured to include the new device after the device is added.

A managed device can be converted to a standalone state by reinstalling the device.

You cannot add McAfee DLP Endpoint to McAfee DLP Manager using this procedure.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP Manager appliance, select **System** | **System Administration** | **Devices**.

2 Select **Actions** | **New Device**.

3 Enter the device IP address or host name and the root password.

4 Click **Add**.

5 Click **OK** to confirm or **Cancel** to cancel the registration.

6 To check the status, refresh the page.

When the **Status** icon in the device list to turns green, registration is complete.

Configure standalone McAfee DLP appliances using the Setup Wizard

Use the **Setup Wizard** to perform initial configuration on standalone McAfee DLP Monitor, McAfee DLP Prevent, and McAfee DLP Discover appliances.

Task

1 Open a web browser and connect to the McAfee DLP appliance.

- For an upgrade or re-installation, enter the appliance's configured IP address.
- For a completely new installation, use the computer connected to the management port and enter `https://192.168.1.2`.

2 Log on to the user interface.

The default credentials are `admin`/`mcafee`. After logging on, you are required to change the default password and log on with the new credentials. If you are using the default root password, you must log on to the command line interface to change the root password.

3 Follow the on-screen instructions to complete the configuration. Consider these points:

- The **Hostname** field requires a fully qualified domain name.
- You can adjust the selected policies on the **Policy Activation** page at a later time from the **Policies** page in the user interface.

After initial configuration is complete, you can rerun the **Setup Wizard** from **System** | **Configure** if you want to make additional changes.

Configure servers for McAfee DLP Prevent

The McAfee DLP Prevent configuration depends on whether the appliance processes email or web traffic.

- **Web traffic** — McAfee DLP Prevent automatically accepts ICAP traffic from any web proxy server. No additional configuration is required.
- **Email traffic** — Use this task to configure the MTA servers that McAfee DLP Prevent accepts mail from, and the server that McAfee DLP Prevent forwards processed mail to.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
   - On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 Select the device and click **Configure**.

   The **System Configuration** page appears.

3 In the **Smart Host**, enter the IP address of the MTA server that McAfee DLP Prevent will forward inspected email messages to.

4 In the **Mail Servers** field, enter the IP addresses of any servers that McAfee DLP Prevent will accept email messages from. Separate entries with a comma; do not use spaces.

   If the Smart Host IP address is also in the **Mail Servers** field, you must configure that email server as appropriate to avoid any routing loops.

5 In the **Email Notification** field, add an administrator email address. McAfee DLP Prevent uses this email address to send a test email to verify the connection.

6 Click **Send test mail** to test the smart host connection.

7 Click **Update**.

Link negotiation for McAfee DLP appliances

McAfee DLP appliances and connected devices, such as switches, routers, or firewalls, must be configured to use full duplex.

Guidelines for Fast Ethernet networks

- Configure the McAfee DLP appliance to use 100 Mbps and full duplex.
- Select one of these options for intermediary devices:
  - Configure the device to use 100 Mbps and full duplex.
  - Configure the device to use auto-negotiation and verify that full duplex is negotiated.

Guidelines for Gigabit Ethernet networks

- Configure the McAfee DLP appliance to use either auto-detect, or 1000 Mbps and full duplex.
- Select one of these options for intermediary devices:
  - Configure the device to use 1000 Mbps and full duplex.
  - Configure the device to use auto-negotiation and verify that full duplex is negotiated.

See also

Change link speed on page 329

Testing the system

If your system doesn't appear to be generating incidents after it is installed, you can take steps to verify that your configuration is correct.

Table 7-2 Configuration checklist

Checks	Explanation	Action
Appliance connections complete	Status icons display health of each managed appliance.	On the **System** page, verify that the **Status** icon is green. If the status is **Registering** or **Unknown**, wait until the process is complete. You might need to refresh the page.
Policies activated	If policies are not activated during the setup phase, their rules cannot be matched to network data.	On the **Policies** page, check the **State** column. If policies are inactive, select policy boxes, then select **Activate** from the **Actions** menu.
Timestamp filter set	The default is **Previous 24 hours** to keep the system from producing unmanageable numbers of results.	On the **Incidents** page, set **Filter by** to a longer time period. If the system was recently installed, it will need some lead time for data capture and analysis.
Capture filters set	The system might have been set up to ignore traffic that is needed to meet your protection strategy. For example, the *RFC 1918* filter blocks internal IP addresses.	On the **System** | **Capture Filters** page, remove filters that might be blocking traffic.
Common keywords producing results	If data is being captured, you will be able to find keywords that are commonly found in your network traffic — for example, your company name.	On the **Basic Search** page, type in a common keyword that can be found in captured data.
Changing the dashboard view displays different results	When using McAfee DLP Manager, the **Data-in-Motion**, **Data-at-Rest**, and **Data-in-Use** dashboards display results in network traffic, repositories and endpoints.	On the **System** page, verify the corresponding products are installed.
Existing filters blocking significant results	When filters are set, only the configured results are visible on the dashboard.	On the **Incidents** page, click **Clear All** in the **Filter by** frame.

Additional tasks

After installation is complete, begin configuring your McAfee DLP appliance to suit the needs of your network protection strategy.

McAfee recommends performing these tasks to complete your deployment.

- Create policies and rules to detect potential violations within your network.
- Add authentication servers to extend the amount of information McAfee DLP produces.
- Create capture filters to exclude data that does not need analysis.
- Schedule disaster recovery backups at regular intervals.

See also

How policies and rules can be used on page 89
Using external authentication servers on page 65
How capture filters work on page 313
How the backup and restore process works on page 339

System configuration

Chapter 8 *Integrating network servers*
Chapter 9 *Administrator accounts*

8 Integrating network servers

McAfee DLP supports several types of servers that extend the functionality of the product suite.

Contents

- *Using external authentication servers*
- *Using McAfee Logon Collector*
- *Using DHCP servers*
- *Using NTP servers*
- *Using syslog servers*

Using external authentication servers

The ability to monitor user traffic on Active Directory servers now has been extended to directory servers, making global user management a reality.

The ability of McAfee DLP to connect to multiple domain controllers makes it possible to capture data on local networks and up to two LDAP servers.

When users can be recognized by name, group, department, city or country, a McAfee DLP administrator can extract a great deal of significant information by using a few seminal facts to gradually gather more details about potential violations.

OpenLDAP and Active Directory server differences

McAfee Data Loss Prevention supports OpenLDAP as well as Active Directory servers.

OpenLDAP and Active Directory produce different user schemas. Active Directory has a constrained set of parameters, but OpenLDAP is completely customizable, so user implementations might vary widely.

OpenLDAP and Active Directory servers identify users by using different means of user identification. Active Directory uses *sAMAccountName*, and OpenLDAP uses *UID*. LDAP queries for sAMAMccountName are handled by using the UID property on OpenLDAP systems.

OpenLDAP and Active Directory servers also identify user classes by using different user attributes. Instead of the User object class, OpenLDAP uses *inetOrgPerson*, which does not support country or "memberOf" attributes.

How directory server accounts are accessed

Historically, McAfee DLP Manager has been linked to sAMAccountName as the main user identification element. But if that attribute is applied to users in the same domain who have similar or matching user names, they cannot be identified conclusively.

McAfee DLP keys on the unique alphanumeric SID (Security Identifier) that is assigned to each user account by the Windows domain controller.

Because McAfee Logon Collector allows McAfee DLP to key on SIDs (Security Identifiers), the identities of individual users can be resolved and their traffic can be monitored. By leveraging multiple user attributes, it is now possible to identify end users precisely, regardless of what email or IP addresses they are using.

When a SID is retrieved from the Active Directory server, all of its associated attributes, such as domain name, location, department and user group, come with it. That collection of information can then be used in rules, templates, action rules, and notifications to find and stop security violations by specific users.

For example, the user name jsmith might belong to John Smith or Jack Smith, so more information would be needed to distinguish between those two users. They might even be using the same IP address, which would amplify the problem of discovering the identity of the actual user.

Each account on an Active Directory server is made up of attributes that identify the individual who owns the account. McAfee Logon Collector matches the unique SIDs that are assigned to each Active Directory user to IP addresses, and all of the parameters associated with that SID are extracted when McAfee Logon Collector moves binding updates from the Active Directory server to McAfee DLP.

Because sAMAccountName was used to index data in earlier releases, that information might be lost during ad hoc searches when the user upgraded, or the data residing in the capture database pre-dates the upgrade.

How directory servers are used with DLP systems

If a directory server is added to McAfee Data Loss Prevention Manager, DLP can use the data on the server to identify remote users and manage their data.

Directory servers enable enterprise users to locate users through their logins, email or IP addresses, or by compound rules that combine user logins with locations or affiliations.

How LDAP user accounts are monitored

Historically, DLP Manager has been linked to sAMAccountName as the main user identification element. But if that attribute is applied to users in the same domain who have similar or matching user names, they cannot be positively identified.

McAfee Data Loss Prevention now keys on the unique alphanumeric SID (Security Identifier) that is assigned to each user account by the Windows domain controller.

For example, the user name `jsmith` might belong to John Smith or Jack Smith, so more information would be needed to distinguish between those two users. Those individuals might even be using the same IP address, which would aggravate the problem of discovering the identity of the actual user.

But each account on an Active Directory server is made up of attributes that identify the individual who owns the account. McAfee Logon Collector matches the unique SIDs that are assigned to each Active Directory user to IP addresses, and all of the parameters associated with that SID are extracted when McAfee Logon Collector moves binding updates from the Active Directory server to DLP.

Because sAMAccountName was used to index data in earlier releases, that information might be lost during ad hoc searches when the user has upgraded, or when the data residing in the capture database pre-dates the upgrade.

Monitoring LDAP users

The ability to monitor user traffic on LDAP servers has extended the reach of McAfee DLP tools to directory servers used by enterprise-sized organizations. Connections through multiple domain controllers makes this possible.

Data on local networks is captured and the software extends this capability to all traffic on up to two remote LDAP servers.

When users can be recognized by name, group, department, city or country, a DLP administrator can extract a great deal of significant information by using what little information is known about those users to gradually gather more details about a potential threat.

For example, suppose you know that your company has lost intellectual property to a Chinese firm, and you suspect that the leak came from an insider in your Shanghai branch.

Because McAfee DLP Monitor captures all traffic on your company's network, you can add an Active Directory server that contains the user account of that insider to McAfee DLP Manager, then search for the UserName of that individual and monitor his communications.

You might then search his communications for the name of the lost component, then find the email address and geographical location of users outside the company who might have received the information. You might not know what will be in those communications, but you can use what you find to form the next question.

Add Active Directory servers

Active Directory or OpenLDAP directory servers must be added to support integration with existing user systems. After the server is configured and users are added, incidents can be detected through user accounts on the servers.

More than one directory server can be added to McAfee DLP Manager, but they must be of the same type. If an Active Directory server is added, you cannot also add an OpenLDAP directory server.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config**.
- On your McAfee DLP appliance, select **System**.

2 Select **System Administration** | **Directory Services**.

3 From the **Actions** menu, select **Create Directory Server**.

4 Type in a label to identify the LDAP server.

5 Do one of the following:

- In the **Domain** field, enter the domain of the LDAP server.

  If you use this option, you must log on to an administrative account on the LDAP server. The system will then query DNS to find the domain controller for the Active Directory domain.

- In the **Authorization Server** field, enter the name or IP address of the Active Directory or LDAP server.

  If you are using SSL (Secure Sockets Layer) to encrypt the connection, you must enter the FQDN (fully qualified domain name) cited in the uploaded certificate.

  Unlike the LDAP server domain name, you can use any valid account that has permission to read from the LDAP server (an administrative account is not necessary). If you have already entered the domain name of the LDAP server, any information you enter here will be ignored.

6 In the **Server Port** field, enter the port for the connection.

7 Set intervals for connection timeout and retries (in seconds).

8 In the **Loginid Attribute**, enter the attribute.

Use `samaccountname` to retrieve user names from the server.

9 In the **Login DN** field, enter the username, then specify a password in the **Password** field.

10 Identify the local domain components in the **Base DN** field (for example, `dc=mydomain,dc=com`).

Use an administrative account whose password does not expire to maintain the connection, but a non-administrative account name is acceptable when using an authorization server.

11 Type in the number of records you want to retrieve at one time in the **Server Results limit** field.

Before entering a value higher than 10, consult the administrator of the Active Directory server to find out how many records can be served per request.

12 Select the **SSL** checkbox to encrypt the connection and enable LDAPS (LDAP over SSL).

A secure connection is not required, but is strongly recommended. Accept any available certificate, or select one by uploading it. If you upload, you must find the FQDN name of the authorization server in the encrypted file by logging on to the back end of the McAfee DLP appliance and running the following.

```
# openssl x509 -noout -in <filename>.cer -subject
```

The FQDN will be returned in reverse order:

```
subject= /DC=net/DC=reconnex/CN=tyche
```

Read from left to right to get the name of the authorization server:

```
tyche.reconnex.net
```

Type the name into the **Authorization Server** field.

13 Select a scope to set the directory depth to be accessed on the server.

14 Click **Apply**.

Add Active Directory or OpenLDAP users

LDAP user accounts can be retrieved from the directory server, or account credentials can be added through McAfee DLP Manager.

Before you begin

New LDAP users must be assigned to existing domains.

Although user accounts can be added directly through McAfee DLP Manager, existing user accounts need not be added to the system. The system retrieves users automatically, and starts detecting incidents through existing accounts.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Users**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Users**.

2 From the **Actions** menu, select **Create LDAP User**.

The **Add New LDAP User** page appears.

3 Add or retrieve users is one of the following ways.

- Type in a known **Login ID** or **User Name**.
- Type in an asterisk (*) to retrieve a list of all users on the server.
- Use an asterisk (*) as a metacharacter to retrieve related users (for example, R* or *st*).

4 Click **Find**.

5 Select one or more users from the list.

6 Select one or more groups from the **Available** groups for the new user and **Add** the users to the groups.

7 Click **Apply**.

To make changes to the user's status later, click **Details** for the user's account.

For example, you can use the **Action** menu to **Disable** or **Delete** the user.

Export certificates from Active Directory servers

Export certificates from Active Directory servers to secure the connection to McAfee DLP Manager.

This task retrieves a certificate from a Microsoft Active Directory server, exports it, and adds it in the McAfee DLP Manager interface.

By default, LDAP traffic is transmitted unsecured, but using secure LDAP over SSL technology encrypts the connection.

Task

1 Log on as a member of one of the following:

- The local Administrator security group for standalone computers
- A member of the Domain Administrator security group for any computers that are connected to the domain.

2 Install the certificate on the Windows server, which will install the server certificate on the Active Directory server.

3 Start the Microsoft Management Console by clicking **Start** | **Programs** | **Administrative Tools** | **Certificate Authority**.

4 Select the CA system, then right-click and select **Properties**.

5 From the **General** menu, select **View Certificate**.

6 Select the **Details** view.

7 Click **Copy to File** on the lower right corner of the window.

8 Use the **Certificate Export Wizard** to save the CA certificate in one of the following formats:
- DER Encoded Binary X-509 format
- Base-64 Encoded X-509 format

9 Verify that SSL is enabled on the Active Directory server:
- Windows 2000
- Windows 2003

a Ensure that **Windows 2000 Support Tools** (**Windows Support Tools** on Microsoft Windows 2003) is installed on the Active Directory server.

b Find the `suptools.msi` setup program in the `\Support\Tools\` directory on your Windows CD.

c Start the ldp tool.

For Microsoft Windows 2000 systems, select **Start** | **Windows 2000 Support Tools** | **Tools** | **Active Directory Administration Tool**. For Windows 2003, select **Start** | **Windows Support Tools** | **Tools** | **Command Prompt**.

10 Select **Connection** | **Connect** from the ldp window.

11 Enter the host name and port number (secure port 636 is required).

If the connection is successful, a window is displayed listing information related to the Active Directory SSL connection. If it is unsuccessful, restart your system and repeat the procedure.

How ADAM servers extend McAfee DLP Manager

ADAM (Microsoft Active Directory Application Mode) servers allow McAfee DLP Manager to access objects in customized database schemas. Default attribute mappings are modified to recognize the names of equivalent fields in existing LDAP databases.

McAfee DLP products enable retrieval of information from Microsoft ADAM servers, making it possible to customize existing attributes to map to McAfee DLP settings.

Use of a Certificate Authority supports secure transmissions through LDAPS or HTTPS. Verification can be disabled by selecting **Accept Any Certificate** when adding the server.

Whenever SSL communication is requested, the host name should be name of the server with domain clearly specified. An IP address will not work.

Mapping default to custom attributes

Default attributes can be mapped to existing databases with different sets of attributes to customize retrieval of records from LDAP servers.

When existing attributes are remapped, incidents reported to the dashboard contain the user information found in the corresponding fields on the existing LDAP server.

Table 8-1 Default attributes

Default attributes
UserName=cn
UserID=sAMAccountName
UserTitle=title
UserCompany=company
UserDepartment=department
UserCity=givenName
UserZipcode=postalCode
UserCountry=countryCode
UserManager=manager
UserGroups=memberOf
UserEmail=proxyAddresses

Using Active Directory attributes

Active Directory attributes can be used for queries and rules, but incidents that are reported on the dashboard might have more objects available in the database. That information can be viewed by adding columns that can display those fields.

All Active Directory elements are treated as word queries, and can be directed to specific LDAP servers. When Active Directory elements are used in a query, columns supporting the parameter are configured in the search pop-up and on the dashboard.

Each of the user elements retrieves the following attributes.

- User Name: user's name, alias, department, location
- User Groups: user's group
- User City: user's city
- User Country: user's country
- User Organization: user's company or organization

Viewing Active Directory incidents

All Active Directory incidents are reported to the dashboard.

When Active Directory elements are used in a query, columns supporting the parameter are configured in the search pop-up and on the dashboard.

When you get results from querying a directory server, you can view them on the **Data-in-Motion** dashboard or the corresponding ePolicy Orchestrator dashboard. Clicking the **Columns** icon will show you what other data categories are available for display.

Not all of these parameters can be used for queries. This accounts for the disparity of data categories on search and rule pages.

Search for user attributes in LDAP data

If a directory server is registered to McAfee DLP Manager, you can search the imported data to find incidents by keying on user attributes.

Directory server data can be searched by source or destination IP and/or port.

Use **Basic Search** to do exploratory searches, and **Advanced Search** to create complex searches or rules.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Click either **Basic Search** or **Advanced Search**.

3 From the **Basic Search** | **Input Type** or **Advanced Search** | **Source/Destination** menu, select a user attribute.

4 Click **Search** or **Save as Rule**.

Find user attributes in LDAP data

If a directory server is registered to McAfee DLP Manager, you can use the imported data to find incidents by keying on the user attributes.

Before you begin

One or more dashboards must display incidents retrieved from a directory server attached to the McAfee DLP system.

Use the filtering process to locate user attributes in dashboard results.

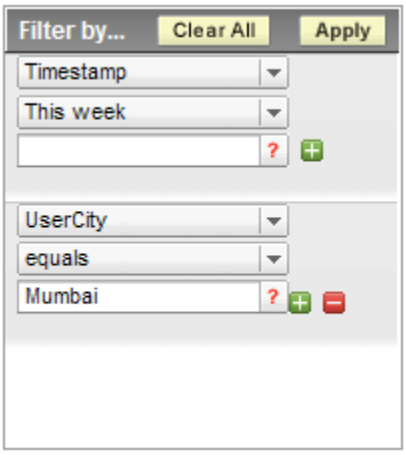


Figure 8-1 Filter for user attributes

Before filtering, add columns to the dashboard to display the user attribute results you are looking for.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 At the top of the **Incidents** page, select a vector: **Data-in-Motion**, **Data-at-Rest**, or **Data-in-Use**.

These dashboards display incidents or events from McAfee DLP Monitor, McAfee DLP Discover, or McAfee DLP Endpoint, respectively.

3 In the **Filter by** pane, select a time frame.

4 Click **+** to add a filter.

5 From the filter list, select a user attribute from the list.

If customized attributes are used on the directory server, they must be mapped to those in this list.

6 Select a comparator, such as **equals** or **not equal**, and enter required information in the value field.

7 Click **Apply**.

LDAP columns available for display

The columns available reflect the scope of data available. Not all of these parameters can be used for searching captured data or implementing rules. In an ad hoc search, some Active Directory attributes (user names, companies, email, managers, titles) are not displayed.
There are many more columns available than there are searchable network elements — many were added to the McAfee DLP product suite interfaces to support McAfee DLP Endpoint. You can use them to display additional attributes that are reported, but not displayed by default.

The following columns are available.

- User Custom
- UserCity
- UserCompany
- UserCountry
- UserEmail
- UserGroups
- UserID
- UserManager
- UserName
- UserGroup
- UserOrganization
- Network printer
- Network path
- Location Tag Path

Add columns to display user attributes

Add columns to display the relevant user attributes that were retrieved from your directory server. The columns available reflect the scope of data that might be available on the directory server. Not all of these parameters can be used for searching captured data or implementing rules. In an ad hoc search, some attributes (user names, companies, email, managers, titles) might not be displayed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click **Columns**.

3 From the **Available** list, select the relevant user attributes.

If customized attributes are used on the directory server, they must be mapped to those in this list.

4 Click **Add** to move them to the **Selected** box.

5 Select the navigation buttons to determine the placement of the user attributes in the dashboard display.

6 Click **Apply**.

Using McAfee Logon Collector

McAfee DLP products use McAfee Logon Collector servers to identify remote users definitively.

With McAfee Logon Collector, remote users are identified through SIDS (Security Identifiers) instead of IP addresses, host names, or other user parameters that are subject to change.

Connect McAfee Logon Collector to McAfee DLP Manager

Connect McAfee Logon Collector to McAfee DLP Manager by using certificates to authenticate them to each other. When the process is concluded, an SSL connection is established between the servers.

Task

1 Open a web browser, type the IP address of the McAfee Logon Collector into the address bar, and logon.

2 From ePolicy Orchestrator, select **Menu** | **Configuration** | **Server Settings** | **Identity Replication Certificate**.

3 Select and copy all text in the **Base 64** field and paste it into a text editor.

4 Add the following beginning and ending lines to the document.

```
-----BEGIN CERTIFICATE-----
<pasted Base 64 field text>
-----END CERTIFICATE-----
```

5 Highlight and copy the entire text, including the BEGIN and END CERTIFICATE lines.

6 Open a web browser and logon to the Network McAfee DLP Manager.

7 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Directory Services**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Directory Services**.

8 From the **Actions** menu, select **Create McAfee Logon Collector**.

9 Type the IP address of the McAfee Logon Collector into the **IP Address** field.

10 Select the **Paste from Clipboard** option and paste the Base 64 text into the box.

Alternatively, you can export the certificate from McAfee Logon Collector to your desktop, then **Browse** to it from the **Import MLC Certificate** | **From File** field.

11 Click **Apply**.

This authenticates the McAfee Logon Collector to McAfee DLP Manager.

12 Click the **Export** link to save the NetDLP certificate to your desktop.

The file name is netdlp_certificate.cer.

13 Open a web browser, enter the IP address of the McAfee Logon Collector in the address bar, and log on.

14 Select **Menu** | **Configuration** | **Trusted CA**.

15 Click **New Authority**.

16 Browse to the netdlp_certificate.cer file you saved to your desktop.

17 Click **Open**, then **Save**.

This authenticates McAfee DLP Manager to McAfee Logon Collector.

18 Open a Remote Desktop session on the McAfee Logon Collector server and restart it.

When the server comes up, the SSL connection between the servers is complete.

How McAfee Logon Collector enables user identification

McAfee Logon Collector is used to map IP addresses to user identities within Active Directory servers. Without it, users might be hard to identify because they might be logged into different or multiple workstations. IP addresses change when DHCP servers assign new addresses, and more than one user might be logged on to the same workstation.

When a McAfee Logon Collector is configured with McAfee DLP Manager, it resolves user identities by retrieving collections of user account information from all Active Directory servers that have been added to the DLP system. Supporting multiple domain controllers means that large-scale enterprise operations can be served by McAfee applications.

For McAfee DLP, that means that after McAfee Logon Collector is enabled, McAfee DLP administrators can configure Active Directory-based queries and rules to find out what activities specific users are engaging in on the network.

How McAfee DLP uses SIDs

Because McAfee Logon Collector allows McAfee DLP to key on SIDs (Security Identifiers) instead of sAMAccountnames, the identities of individual users can be resolved and their traffic can be monitored. By leveraging multiple user attributes, it is now possible to identify end users conclusively, regardless of what email or IP addresses they are using.

When a SID is retrieved from the Active Directory server, all of its associated attributes, such as domain name, location, department and user group, come with it. That collection of information can then be used in rules, templates, action rules, and notifications to find and stop security violations by specific users.

Using DHCP servers

McAfee DLP can accurately resolve the sources and destination of network transmissions by using DHCP (Dynamic Host Configuration Protocol) services. A DHCP server might be added to the system to provide those services.

Senders and recipients can be easily identified if they have static IP addresses, but dynamic addresses are more commonly used. Because they change frequently, it is often difficult to pinpoint the sources and destinations of transmissions.

DHCP servers automatically assign IP addresses from an appropriate pool to the clients connecting to the system. The server then extracts, parses and loads log files to resolve the address to a host name, and the information is passed along to the DLP system.

If McAfee Logon Collector is used with an Active Directory server, user mapping returns better results.

Add DHCP servers to DLP systems

Add DHCP (Dynamic Host Configuration Protocol) servers to DLP systems to provide accurate location information about incidents that have been identified by DLP systems. If there is no Active Directory server, DLP processes query the DHCP server to map IP addresses to users.

DHCP servers are used by most ISPs (Internet Service Providers) to assign dynamic addresses to the hosts they administer. Because dynamic addresses expire at specified times, hosts using them can be tracked only through DHCP server records.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **DHCP Servers**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **DHCP Servers**.

2 From the **Actions** menu, select **Add DHCP**.

3 Type in a name for the server and an optional description.

4 Select the server type.

Internet Systems Consortium, Solaris and Microsoft Windows types are supported.

5 Select an access mode to retrieve directory information, get and put log files, and perform related transfer tasks.

The access mode determines the method of transfer. SMBClient access mode is supported only for Windows Server.

6 Type in the IP address or host name, the username, and the password to log on to the server.

7 Type in the folder or share name, if needed.

8 Add the file name or pattern to enable DHCP logging.

The DHCP log file name depends on the DHCP server operating system. `DhcpSrvLog` is a Windows file name pattern. Use `dhcpd*` for ISC and Solaris DHCP logs (`dhcpd.leases`).

Matching this pattern enables DHCP logging. For the SMB client, `mget DhcpSrvLog*` can be used from the SMB prompt to link to Windows files such as `DhcpSrvLog-Wed.log` or `DhcpSrvLog-Sun.log`. For SCP or SFTP, use `/var/state/dhcp/dhcpd.leases` or `/var/state/dhcp/dhcpd*`.

9 Set the frequency to indicate how often the server should be polled to pull down new information.

10 Select the checkboxes of devices to be connected to the DHCP server.

11 Click **Save**.

Using NTP servers

McAfee DLP can use NTP (Network Time Protocol) to synchronize the system clock.

Correct time in the McAfee DLP Manager interface

Correct time settings in the McAfee DLP Manager interface to re-synchronize with the network.

This procedure might clear the synchronization error message displayed when logging on. If this doesn't work, log on to the back end as root and reset the time from the McAfee DLP Monitor command line.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 Click the **Configure** link for a specific device.

3 Scroll down to **Time** and select **Manual**.

4 Enter the correct date and time.

5 Click **Update**.

6 Log out of McAfee DLP Manager, then log on again.

Synchronize McAfee DLP devices with NTP servers

Synchronize McAfee DLP devices with network time servers if they lose their connections to the network.

Use this task to re-synchronize McAfee DLP device time with your desktop.

This is one way to clear a system time error that might prevent you from logging on.

Task

1 Open the **Date/Time** display on a Windows desktop.

2 Adjust local time to Greenwich Mean Time.

3 Log on as root to the McAfee DLP appliance.

4 Type the date - -utc command to enter the correct date and time.

```
# date --utc MMDDhhmmCCYY
```

5 Type the hardware time command to reset the clock.

```
# hwclock -w
```

6 Type the date command.

```
# date
```

7 If the correct date is returned, reset Stingray.

```
# service stingray reset
```

8 Find and kill the current process.

```
# ps -ef | grep java
# kill -9 <process id number>
```

9 Log on again as root to the McAfee DLP appliance.

10 Restart Stingray and reboot the machine.

```
# service Stingray restart
# reboot
```

11 Open a web browser and enter the address of the McAfee DLP appliance in the address bar.

12 Return the Windows clock setting to the correct time zone.

Reset time manually

Reset time manually by stopping and restarting NTP services.

Stop and restart the NTP daemon to manually reset the time.

Task

1 Log on as root to the McAfee DLP appliance.

2 Stop the NTP daemon.

```
# service ntpd stop
# chkconfig --level 2345 ntpd off
```

3 Restart the NTP daemon.

```
# service ntpd start
 # chkconfig --level 2345 ntpd on
```

The service command will control the service while the system is running; the `chkconfig` commands will control what happens at boot time.

Using syslog servers

Syslog servers are automatically recognized if they reside on the same network as McAfee DLP devices; no special connection is needed. If a syslog server is installed on the network, McAfee DLP automatically sends messages about significant events in the following format.

The health of the McAfee DLP appliances, as well as the rule hits, are automatically transferred to the syslog server.

Table 8-2 Syslog server message definitions

Message field	Definition
Date	Date the event was logged
Host name	Name or IP address of the machine that logged the event
Component	Component or process that generated an alert
Format	Format version of the syslog output
Device vendor	Vendor name
Device product	Manager, Monitor, Discover, Prevent or Endpoint
Device version	Product version
Rule	Search rule
Severity #	Critical, High , Medium, Low, Informational
Policy	Policy name
Policy label	Type of object
Match count	Matches found
Match count label	Type of object
Source IP	Source IP address

Table 8-2 Syslog server message definitions *(continued)*

Message field	Definition
Destination IP	Destination IP address
Source Port	Source port
Destination port	Destination port
Source user name	Source user name
Destination name	Destination user name
Email subject	Email subject
File name	File name

9 Administrator accounts

McAfee DLP users inherit their privileges from group membership. The system is based on Role-Based Access Control (RBAC), which is used to assign access to users based on the privileges they need to execute their assignments.

Administrators can assign users to the role-based groups installed on McAfee DLP Manager, customize those groups, or add new groups. They can also create system or ePolicy Orchestrator database users locally on McAfee DLP Manager, or imported user accounts from LDAP servers.

The primary administrator of a McAfee DLP Manager has all privileges needed to grant access to users and groups, and can assign those rights to other administrators.

Administrators can create failover accounts to allow access if a system component goes down. They can also audit user activity, save user logs, or customize their logins and passwords.

Contents

- *Managing user accounts*
- *Managing user groups*
- *Managing permissions*

Managing user accounts

User account types can be reconfigured to assign different privileges, customize login and password settings, or change the account type.

Administrators can customize login and password settings for local users, configure different types of administrator account, or add configure failover accounts if needed.

Configure primary administrator accounts

Configure additional administrator accounts if you are the primary administrator. Do this immediately after the first login to preserve the integrity of the default account.

Primary administrators have complete access to all task and policy permissions and are responsible for creating users and custom user groups. Dividing responsibilities by allocating specific tasks to additional administrators is recommended.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Click **Details** for the **Administrator** group.

3 Edit the **Group Name**, **Description**, and **Email** address as required.

4 From the **Available Users** menu, select the users to be added to the group.

5 Click **Apply**.

Activate a failover account

Failover accounts allow back door access to McAfee DLP Monitor and McAfee DLP Manager in case the system goes down.

If the link between McAfee DLP Manager and McAfee DLP Monitor is open, the default failover account could be used to logon to the system, so failover accounts are disabled by default.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Failover Account**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Failover Account**.

2 In the **Login ID** field, enter the user name for the failover account administrator.

3 Enter a password for the failover account administrator.

4 Set **Allow Login** to **On**.

5 Click **Update**.

Customize logon settings

Customize logon settings to discourage unauthorized logons. Lockout is disabled by default, but should be enabled to prevent cracking attempts.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **User Settings**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **User Settings**.

2 Select the **Enable lockout** box.

3 Enter the maximum number of failed attempts allowed.

4 Set the **Mode of disabling lockout** to **Automatic** or **Manual**.

5 Set the time frame (in minutes) to reset logon for locked-out users.

6 Click **Submit**.

Customize password settings

Customize password settings to discourage unauthorized logins.

Lockout is disabled by default, but should be enabled to prevent cracking attempts.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **User Settings**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **User Settings**.

2 Type in the minimum and maximum length of characters allowed for passwords.

3 Type in the minimum number of upper- and lowercase alphabetic, numeric and special characters to be allowed.

4 Click **Submit**.

Managing user groups

McAfee DLP systems user Role-Based Access Control (RBAC) to match the rights of individual users to their roles, which are defined by user group permissions.

Administrators can utilize the default pre-configured groups, edit them, or create new groups as needed.

Add user groups

Add user groups to define user roles, and assign permissions to the groups that propagate to the users who are group members.

Permissions that are checked on the **Task Permissions** and **Policy Permissions** pages affect what is displayed in the user interface.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 From the **Actions** menu, select **Create New Group**.

Alternatively, select **Details** and rename a pre-configured group.

3 Type in a group name and optional description.

4 Type in an email address for the group.

5 From the **Available Users** box, select users and add them to the **Current Members** box.

Remove users as needed.

6 Click **Apply**.

7 Click the **Task Permissions** tab, open each category, and select the checkboxes of task permissions to be assigned to the group.

View Dashboard permission is required to see the **Incidents** dashboard.

8 Click **Apply**.

9 Click the **Policy Permissions** tab, open the **Policies** category, and select the checkboxes of permissions for each policy to be assigned to the group.

10 Click **Apply**.

Delete user groups

Delete user groups that are not needed or no longer useful. Only administrators can delete user groups.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Click **Details** for the group to be deleted.

3 From the **Action** menu, select **Delete** and click **Go**.

4 Click **OK** to delete the group.

Managing permissions

Permissions are assigned through group membership. Administrators can customize group permissions by adding specific policy and task permissions that individuals need to perform their tasks.

Assign incident permissions

In a role-based access control systems, not all users have privileges to view all types of incidents produced by the McAfee DLP system.

For example, as a member of the group responsible for reviewing evidence of non-compliance with SOX policy, an accountant might have access only to incidents produced by the rules of that policy.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Users**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Users**.

2 Click **Details** for a user.

3 Click **Incident Permissions**.

4 Click **Add**.

5 Select **Reviewer**, **Rule**, or **Devicename** from the drop-down menu.

6 Select an **equals** or **not equals** condition.

7 Click **?**.

A palette containing the values available for the selection appears.

8 Select one or more value checkboxes.

9 Click **Apply**.

Assign task and policy permissions

All user rights are inherited from group affiliations. Assign permissions to individual users by adding them to the appropriate groups.

If group permissions are modified, all of its members will have to log out and re-logon.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Click **Details** for a group.

3 Click **Task Permissions**, open each category, and select permissions.

4 Click **Apply**.

5 Click **Policy Permissions**, open each category, and select permissions.

6 Click **Apply**.

Check user permissions

Check user permissions to determine access to McAfee DLP features. Because all rights are inherited from group affiliation, users must determine their group affiliations first.

This procedure works only if an administrator has given the user's group permission to view permissions.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Select **Details** for the group.

3 Click **Task Permissions**, open each category, and view the boxes of task permissions assigned to the group.

4 Click **Policy Permissions**, open each category, and view the boxes of policy permissions assigned to the group.

Check group incident permissions

Check group incident permissions to determine the dashboards the members of a group can see, and the features they can use.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Click **Details** for the group.

3 Click **Task Permissions**, open **Incident Permissions**, and view the permissions assigned to the group.

Policy configuration and data use

Chapter 10 *Policies and rules*
Chapter 11 *Rule elements*
Chapter 12 *Policy configuration options*
Chapter 13 *Integrating McAfee DLP Endpoint*
Chapter 14 *Scanning databases and file repositories*
Chapter 15 *Incident dashboards and reports*
Chapter 16 *Case management*
Chapter 17 *Searching captured data*
Chapter 18 *Capture filters*

10 Policies and rules

Policies are made up of groups of related rules that are matched to data and events in network traffic and repositories. When a rule matches on an object within the rule definition, an incident is generated and reported.

Related rules are collected in policies that target specific issues. Many standard policies are pre-installed on McAfee DLP, and users can choose which ones to activate and deploy. For example, the *Payment Card Industry* policy contains four rules. Two contain concepts that use regular expressions with algorithms to match any type of credit card number, and two monitor the data contained in magstripes.

After McAfee DLP has captured and processed data for some time, violations that are found by the rules under standard policies are reported to the **Incidents** dashboard.

When McAfee DLP Endpoint is deployed as a standalone product, all of its deployed rules are managed by a single global policy. When it is installed as part of the McAfee DLP product suite, its global policy is woven into the unified policy design, and the global policy is implicit (it is not visible on the McAfee DLP dashboards as a separate entity). Violations are reported as events that can be viewed on the **Data-in-Use** dashboard.

Contents

- *How policies and rules can be used*
- *Managing policies*
- *Managing rules*
- *Refining rules*
- *Typical scenarios*

How policies and rules can be used

Policies and rules can be used to analyze trends and customize your protection strategy. You can also use existing policies by modifying their parameters.

Analyzing trends in data matching

You can analyze trends in data matching by using the **Chart** and **Compare** features on the **Edit Policy** and **Edit Rule** pages.

By checking these graphical aids for each of your active policies, you can easily analyze the trend of the rule hits and the number of matches found by each rule, and tune them if they are not producing significant results consistently.

Alternatively, you might want to use these charts to monitor matches based on their importance to your protection strategy. For example, if it is essential to monitor all intellectual property and compliance-related incidents, but Human Resources violations are not considered high-risk incidents, they might be checked only when their match count exceeds a certain threshold.

Use Chart and Compare to prioritize policies

You might deploy many policies that produce useful results, but some might be more important than others. You can use the **Chart** and **Compare** features to determine when a low priority policy generates hits, which of its rules produce the most matches, and monitor the violation count over time.

When the match count produced by a low-priority policy trends upwards, you might put measures in place that will allow you to address all violations produced by a single rule. For example, if the *Discrimination in Email or Chat* rule in the *Acceptable Use* policy starts producing an inordinate number of matches, you might add an action to the rule that assigns all future matches to your legal team for investigation.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Open a low-priority policy and click **Chart** on the **Edit Policy** page.

The daily, weekly, and monthly trend charts appear.

3 If any of the charts shows a trend in when matches occur, close the chart and click **Compare** to compare the number of hits with those found by other policies.

The **Comparison** chart appears.

4 When you determine which policy is producing the most matches, open one of its rules and click **Compare** to find out which of its rule is firing most frequently.

5 Open the active rule and click **Actions**.

6 Click **Add Action**, and click on the most appropriate *Assignment* action rule.

7 Click **Save**.

When the rule finds a match, it will automatically route the incident to users who can resolve it.

Use Chart and Compare to tune policies and rules

When a policy is deployed for the first time, the efficacy of its rules is unknown. You can use the **Chart** and **Compare** features to determine when the policy's rules hit, and which rules produce the most useful matches. You can then tune and test rule parameters until you get significant and reliable results. While you are searching captured data to which rule parameters work best, suppress incidents to bypass reporting to the dashboards. Even though matches are not reported, each one is stored in the **Data-at-Rest** or **Data-in-Motion** databases, and reporting can be restored after the modified policy and its rules are redeployed. When the process is complete, all parameters should be producing reliable results.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Select a policy that contains rules that need to be tuned.

3 On the **Edit Policy** page, select the **Data-at-Rest** or **Data-in-Motion** checkboxes in the **Suppress Incidents** section.

4 Click **Chart** to find the time frame in which the policy's rules are reporting matches.

5 Click **Compare** to find out which rule is reporting the most matches.

6 After analyzing the rules, apply the parameters of each one against captured data and observe the results.

7 Repeat the process until each parameter is producing useful matches, then modify and re-save each rule.

8 On the **Edit Policy** page, click **Chart** and **Compare** to verify the efficacy of the modified policy and rules.

9 If the results are acceptable, deselect the **Data-at-Rest** or **Data-in-Motion** checkboxes in the **Suppress Incidents** section.

10 Click **Save**.

Managing policies

Policies are containers for groups of rules that monitor conditions related to a single issue.

When an incident is produced by the rules of a policy, the **Group by** window displays the name of the policy that produced it.

Standard policies are installed on McAfee DLP Monitor, McAfee DLP Discover, or McAfee DLP Prevent appliances before shipment. Characteristics like geographic location, industry sector, and business type might determine which ones are active. But customized policies can be created at any time to apply to specific business operations.

There are three basic policy types.

Table 10-1 Policy types

Policy type	Function	Examples
Compliance	Regulatory	SOX, HIPAA, PCI, PII, GLBA, FISMA, ITAR, SB 1386
Intellectual property	Competitive	Customer lists, Price/Cost lists, Target Customer lists, new designs, company logos, source code, formulas, process advantages, pending patents
High Business Impact information	Financial	Board minutes, financial reports, merger/acquisition documents, product plans, hiring/firing/RIF plans, salary information, acceptable use standards

Contents

- *Policy inheritance*
- *Policy activation*
- *Activate or deactivate policies*
- *Add, modify, and deploy policies*

Policy inheritance

Inheritance establishes the relationship of a rule to its policy.

Policies can be in **Active** or **Inactive** states. They are **Inactive** by default, and must be set to an **Active** state before their rules can be matched to data. Rules can also be active or inactive (enabled or disabled), but the state is not set by the user. The **Inherit Policy State** of a rule determines whether it is **Enabled** or **Disabled**.

For example, if the **Inherit Policy State** of a rule is set to **Enabled**, it mirrors the state of the policy, and runs at the same time as the other rules. But if it is set to **Disabled**, the rule does not inherit the state of the policy, whether it is **Active** or **Inactive**.

When a rule is first created, its inheritance state is **Disabled** by default, because it might have to be tested before it is finalized. During the tuning process, a rule must be run, its hits evaluated, and its parameters modified until it produces significant incidents and events. Once it is producing reliable results, its connection to its policy state can be **Enabled** so that all of the policy's rules (assuming the policy is in an **Active** state) can run as a unit.

Policy activation

Policies must be activated before their rules can be applied to network data. By default, rules are enabled when their policies are activated, but they can be configured to run alone.

Policies must also be deployed to at least one McAfee DLP appliance before the system can report incidents and events.

It is not necessary to activate all regional policies at once. For example, United Kingdom users might add the EMEA regional policy package, but activate only the UK policy. Similarly, North American users might want to use only U.S. government regulatory policies, like HIPAA, SOX and ITAR.

There are three ways to activate policies.

- In the **Setup Wizard**, select the checkboxes of the policies to be activated after installation is complete.
- On the **Policies** page, select policy checkboxes and select **Activate** from the **Actions** menu.
- On the **Edit Policy** page, select **Active** from the **State** menu.

Activate or deactivate policies

The rules of a policy will not run unless it is activated. Its rules will not run unless they are enabled. Policies are usually activated during installation, but their states can be reset on the **Policies** or **Edit Policy** pages.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Select one or more policies to be activated.
   - From the **Actions** menu, select **Activate** and verify the change in the **State** column.
   - Click a policy name and select an activation state from the **State** menu.

3 Click **Save**.

Add, modify, and deploy policies

Add, modify and deploy policies to assure efficient performance of the system.

Tasks

- *Add international policies* on page 93
  Add policies that are configured for your region or geographical location.
- *Add policies* on page 94
  Add custom policies to the standard policies that are pre-installed on McAfee DLP appliances.
- *Rename policies* on page 94
  Rename policies to create policies that have the same attributes as the original.
- *Clone policies* on page 94
  Clone a policy to create a new one with the same attributes.
- *Change ownership of policies* on page 95
  Policies can be reassigned to new owners, and the owners belong to user groups that are defined by an administrator.
- *Delete policies* on page 95
  Delete policies in groups or one by one.
- *Modify policies* on page 95
  Modify policies to change owners, devices, and other parameters of policies.
- *Deploy policies* on page 96
  Deploy policies by publishing them to the appropriate McAfee DLP appliances.

International policies

International policies contain rules that monitor local network traffic and repositories for significant regional incidents and events. They monitor privacy data from more than two dozen countries in EMEA, APAC, Latin and North America.

International rules monitor numbering patterns for passports, driver's licenses, governmental and banking entities, and health and social services documents. They include new rules developed for China, Japan, Russia, Korea, and the Czech Republic.

Customized regional policies and rules can also be created at any time to address local issues specific to business operations.

Add international policies

Add policies that are configured for your region or geographical location.

You can easily remove regional policies if the geographic location needed is not on the list.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 From the **Regional Policy Selection**, select a region.

3 Click **Add**.

Click **Remove** if the policies you need are not listed.

Add policies

Add custom policies to the standard policies that are pre-installed on McAfee DLP appliances.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 From the **Actions** policy, select **Add Policy**.

3 Type in a name and optional description.

4 Select an **Owner**.

Standard policies are owned by *admin* by default. If another policy owner is needed but not listed, add the user to a new or existing user group.

5 Set **State** to **Active** if you are going to use the rule immediately. An inactive policy cannot produce incidents.

6 Select **Data-at-Rest** or **Data-in-Motion** if you want to limit the rule to static or dynamic data.

7 Select one or more device checkboxes to publish the policy to specific appliances. Select **None** if you want to publish the policy at a later time.

8 Click **Save**.

The next step is to add rules. You will also want to assign access rights to the policy at **User Administration** | **Groups** | **Policy Permissions**.

Rename policies

Rename policies to create policies that have the same attributes as the original.

None of the incidents and events found by the original policy will be maintained.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 On the **Edit Policies** page, enter a new name and an optional description.

4 Click **Save**.

5 On the **Policies** page, verify that the policy has been renamed.

Clone policies

Clone a policy to create a new one with the same attributes.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a **Policy Name**.

The **Edit Policy** page appears.

3 Type in a new name and an optional description.

The **Save As** button appears.

4 Edit parameters as needed.

5 Click **Save As**.

6 On the **Policies** page, verify that the cloned policy has been added.

Change ownership of policies

Policies can be reassigned to new owners, and the owners belong to user groups that are defined by an administrator.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Select one or more policies in one of two ways.

- From the **Actions** menu, select **Modify Owner**, then select a user group from the sub-menu.
- Click a policy name and select a user group from the **Owner** menu.

3 Click **Save**.

Delete policies

Delete policies in groups or one by one.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Select the policies to be deleted.

3 Delete policies in one of two ways.

- From the **Actions** menu, select **Delete**.
- In the **Delete** column, click the trash can icon of the policy to be deleted.

Modify policies

Modify policies to change owners, devices, and other parameters of policies.

Some policy modifications can be performed from the **Actions** menu.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Change the **Policy Name** or **Description**.

Changing the policy name allows you to **Save** (rename) or **Save As** (clone) the policy.

4 From the **Owner**, **State**, and **Region** menus, make appropriate selections.

5 In the **Suppress incidents** field, select a checkbox to store incident results in one of the available datasets without reporting them to the dashboards.

6 In the **Devices** checkbox, select one or more to publish the policy to the appropriate devices.

7 Click **Save**.

Deploy policies

Deploy policies by publishing them to the appropriate McAfee DLP appliances.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** .
- On your McAfee DLP appliance, select **Policies**.

2 On the **Policies** page, click a policy.

3 On the **Edit Policy** page, select a **Devices** checkbox.

4 Click **Save**.

Managing rules

Rules contain patterns that are matched against data in network traffic and repositories to produce incidents and events. When the rules of a policy detect a significant object, it is saved in a database, then reported to a dashboard.

Standard policies that are pre-installed on McAfee DLP Monitor, McAfee DLP Discover, or McAfee DLP Prevent appliances contain groups of related rules. The rules filed under them are enabled by default so that they will run whenever the policy runs. New rules are disabled by default because their states must be defined before they are used with a policy. Usually they are tuned to assure efficacy before state is defined.

Custom rules can be created at any time to address issues specific to business operations. The system can manage 512 active rules, but if that limit is exceeded, some can be deactivated to allow addition of new rules.

Users' permissions to manage rules depend upon group membership, which must be configured by an administrator.

Add rules

Add rules by searching captured data, then saving the search when it returns reliable results.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Select either **Basic Search** or **Advanced Search**.

3 Enter a query that might retrieve significant results. If significant incidents are reported, do one of the following:

- Click **Save as Rule**.
- Modify the parameters until the needed results are returned, then click **Save as Rule**.

The **Edit Rule** page appears.

4 Enter a rule name and add an optional description.

5 Assign the rule to a policy by selecting one from the **Policy** menu.

Store the new rule in a policy containing rules like it.

6 Select a **Severity** to rate the importance of the rule.

7 In the **Inherit Policy State** area, select the **Enabled** option.

If the rule is to be tuned, leave it in **Disabled** state so it can be run independent of its policy until it reports the needed results reliably.

8 Make any needed changes to the parameters of the rule.

9 Click **Save**.

Find rules

Find existing rules by typing a rule name or keyword into the **Find Rule by Name** field.

The policy that contains the rule you want to find must be listed on the **Policies** page, but need not be active. For example, if you looked for the word `Passport`, but had only Asia Pacific region policies listed, you would find Chinese, but not Canadian passport numbers.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 In the **Find Rule by Name** field, type a rule name or keyword.

For example, to find an Australian driver's license rule, type `Queensland` or `Victoria`.

3 Click **Go**.

View rule parameters

View rule parameters by opening the policy the rule is filed under, then opening the rule.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
   - On your McAfee DLP appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name to open the **Edit Rule** page.

4 Open the categories under the **Define**, **Actions**, and **Exceptions** tabs.

5 If no changes are warranted, click **Cancel**.

Copy rules to policies

Rules can be copied from one policy to another.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name to open a rule.

4 In the **Rule Name** field, enter a new name.

   If a similar name is needed, add a single character or space to distinguish it from the original.

5 (Optional) Type in a new description.

6 Assign the rule to a different policy by selecting one from the **Policy** menu.

   The new rule will be stored in the selected policy.

7 Select a **Severity** to rate the importance of the rule.

8 Set the **Inherit Policy State** to **Enabled**.

   If the rule is to be tuned, leave it in **Disabled** state so it can be run independent of its policy until it reports the needed results reliably.

9 Make any needed changes to the parameters of the rule.

10 Click **Save**.

11 Open the policy containing the new rule to verify that it has been copied over.

Disable rule inheritance

Pre-installed policies contain rules that inherit the active or inactive states of their policies by default. They are designed to act as a group and run whenever the policy runs.

New rules are disabled by default because they have not yet been proved to be effective, and their rule definitions might need modification. After tuning and testing, new rules should be enabled so that they run at the same time as the other rules of the policy.

Clone a standard rule and use its parameters to build a new one. Disable inheritance immediately to disconnect it from the original policy and rule.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name to open the **Edit Rule** page.

4 Change the **Inherit Policy State** parameter to **Disabled**.

5 Click **Save**.

   If the rule needs further definition, consider tuning it until it returns the results you need.

Reconfigure rules for web traffic

Reconfigure rules to monitor web traffic by modifying them to look for HTTP activity.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Select a policy, then a rule that you want to adapt to web traffic.

   The **Edit Policy** page appears.

3 Enter a new name and an optional description.

4 Click **Save As**.

   The **Save As** button appears when you start typing in the name field.

5 In the **Protocol** category, click **X** to delete any existing protocol parameters.

   If there are none, the **X** button is not accessible.

6 Select **Protocol** | **is any of**, then click **?**.

   The **Protocols** pop-up menu opens.

7 From the **Internal Protocols** categories, select the HTTP checkboxes.

8 Click **Apply** and **Save**.

Delete rules

Delete rules individually or in groups.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Click a policy name to open the **Edit Policy** page.

3 Select the rules to be deleted.

4 Delete rules in one of two ways.
   - From the **Actions** menu, select **Delete**.
   - In the **Delete** column, click the trash can icon of the rule to be deleted.

Modify rules

Modify rules to assure their efficacy. Rules can be modified many times, or *tuned*, before they are finalized.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Click a policy name to open the **Edit Policy** page.

3 Click a rule name to open the **Edit Rule** page.

4 Make changes to parameters as appropriate.

5 Click **Save**.

Refining rules

When rules match network data but do not produce useful information, the resulting incident is referred to as a *false positive*. Tuning and adding exceptions to rules that produce false positives identifies the attributes that match irrelevant data, and keeps the classification engine from reporting them to the dashboard again.

Tune rules

Tune rules by testing them on historical data before applying them to data captured in real time. By testing each rule before its policy is applied, you can eliminate parameters that produce false positives.

Click on a policy in the **Group by** window and examine the incidents reported by its rules. Click **Details** for an incident to determine the rule that produced it, then edit the rule to produce better results.

The **Test Rule** button is available only when tuning rules, because the test uses only historical data. The **Tune Rules** button is available on the **Incidents** dashboard or the **Incident Details** page.

During the process, you might want to analyze the performance of the rule by clicking on the **Chart** and **Compare** charts. These tools will help you to understand how the rule results fit into the trend and the performance of the other rules.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click on a rule in the **Group by** window and evaluate its existing incidents.

3 When you find one that is delivering a false positive, click **Details** and make a note of the policy and rule that produced the incident.

You can select all incidents produced by the rule and tune them in a single operation by selecting the **Tune Rule**.

4 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

5 Click on the policy, then the rule.

The **Edit Rule** page appears.

6 Set the **Inherit Policy State** to **Disabled** so you can run the rule without the other rules in the policy.

7 Examine the design of the rule, and determine why it produced the incorrect hit.

If you launch the **Edit Rule** page directly from the **Tune Rule** button on the **Incidents** or **Incidents Details** pages, the **Exceptions** page is populated with the current values of the rule under the tab. You can then modify the values as needed.

8 Change one or more parameters that you think might produce a better result.

For example, if the text pattern of your rule matched all Microsoft Office documents, but you needed only spreadsheet data, deselect **Select All** in the *Office Applications* category to retrieve only Microsoft Excel documents.

9 Click **Test Rule**.

The **Advanced Search** page appears and displays a text report of all of the parameters of the rule.

10 Modify the rule to eliminate the parameters that produced the incorrect results.

The **Advanced Search** page appears, displaying a text report of all of the parameters of the rule.

11 Repeat the process until your rule retrieves the correct results.

12 Click **Save**.

Identify false positives

Identify incidents as false positives by making a note of the incorrect parameters on the **Edit Rules** page. You can tune the rule in the same operation.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.

2 On the dashboard, locate a false positive incident.

3 Identify the incident as a false positive in one of two ways. **Edit Rule**
   - Select the checkbox of the incident and click **Tune Rule**.
   - Click **Details**, then click **Tune Rule**.

4 When **Exceptions** page opens, add a note to the parameter that is producing the false positive.

5 If appropriate, edit the values to redefine the exception.

6 Click **Save**.

Define exceptions

Define exceptions by searching captured data until you find the parameters that work correctly. Then add the useful parameters and the exceptions to a rule.

Eight exceptions are supported for each rule, so you can define precisely the conditions that are not to be matched. The capture engine will drop any incident matching the exceptions.

Exceptions apply to real-time searches only.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Click a policy name, then a rule that needs an exception definition, or add a new rule.

3 Click the **Exceptions** tab.

4 Open **Exception 1**, enter a note describing the exception, then use the components to define the exception you found while searching.

5 If additional parameters are needed, create more exceptions.

6 Click **Save**.

Add new rules with exceptions

Add exceptions to rules to assure that they report only relevant results. When rules contain attributes that are too broad, false positives might be reported.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** .
   - On your McAfee DLP appliance, select **Policies**.

2 Click a policy name to which the rule will be added.

3 On the **Edit Policy** page, select **Add Rule** from the **Actions** menu.

4 Type in a rule name and optional description.

5 Set the **Inherit Policy State** to **Enabled**.

   If the rule is to be tuned, leave it in **Disabled** state so it can be run independent of its policy until it reports the needed results reliably.

6 Select a **Severity** to rate the importance of the rule.

7 Click the **Exceptions** tab.

8 Open **Exception 1** and enter a note describing the exception, then use the components to define the exception to the rule.

9 If additional parameters are needed, open more **Exceptions** and define them.

10 Click **Save**.

Typical scenarios

Standard policies can be used for many common use cases, and they can be easily adapted to fit custom needs.

Protect intellectual property by customizing a standard policy

If you are trying to trace the origin of an intellectual property violation, you might find the source by customizing the rules of the *Competitive Edge* policy.

> **Before you begin**
>
> On the **Policy** page, check the status of the *Competitive Edge* policy. It should be set to **Active**, and all of the rules within it should be **Enabled**.

Depending on what you know about the incident, you can refine the rules in the policy so you can gradually find the source of the problem. Adapt the following suggested parameters to your own systems.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 In the *Competitive Edge* policy, open the first rule.

The **Edit Rule** page appears.

3 Modify the following suggested parameters to adapt the rule to your protection strategy.

- In the **Content** category, select **Keywords contains any of**, then type keywords that might be in your confidential documents.
- Remove the **Common Content Types** template to limit matches to a single content type. In the **Content** category, select **Content Type contains any of**, click **?**, and select a file format from the pop-up menu.
- In the **Source/Destination** category, select **Email Address** | **sender is any of**, then type the email addresses you are targeting into the value field (separated by commas).
- In the **Source/Destination** category, select **UserName** | **sender is any of**, click **?**, and select the directory server that contains the user's account. Click **Find**, select the user, then click **Apply**. If you select **Everyone**, the rule will apply to all users on your directory servers.
- In the **Protocol** category, click **?** and select *FTP* from the **File Sharing Protocols** pop-up menu, then click **Apply**.
- In the **Endpoint** category, select **Protect Local Printers**, **Protect Screen Capture**, select the **Enable** checkbox, and **Apply**.
- In the **Date/Time** category, select **File Last Accessed**, then define the last time a confidential document was accessed.

4 Click **Actions**, **Add Action**, and select the **Print Screen Reaction** or **Printer Reaction** from the **Data-in-Use** menu.

5 After you have finished adding as much information as you have to the rule, click **Save**, let the policy and rule run, and tune as needed.

Identify insider threats by deploying a standard policy

If you are trying to prevent damage from insider threats, you can monitor network traffic using the *Employee Discontent* policy.

> **Before you begin**
>
> On the **Policy** page, check the status of the *Employee Discontent* policy. It should be set to **Active**, and all of the rules within it should be **Enabled**. If you are monitoring insiders who have accounts on a directory server, it should be registered to McAfee DLP Manager.

Depending on what you know about employee morale, you might modify the rules in the policy to target a single business unit — or edit the DISCONTENT concept to include specific language you might expect to find in employee communications.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Concepts**.
- On your McAfee DLP appliance, select **Policies** | **Concepts**.

2 Open the *Acceptable Use* category and click DISCONTENT.

3 Add, modify, or delete expressions using the existing regular expression patterns, then **Save**.

4 In the page header, click **Policies**.

5 Open the *Employee Discontent* policy, then the *Disgruntled Employee Communications* rule.

The **Edit Rule** page appears.

6 Open the **Source/Destination** category and select **User Organization** from the **Elements** menu.

Review the other elements on the menu to focus on specific email or IP addresses.

7 Click **Actions**, then **Add Action** to add more actions, if needed.

The standard rule is set to automatically assign any incidents to Human Resources.

8 Click **Save** and periodically check the **Incidents** dashboard for results.

In the dashboard **Group by** frame, click the **Employee Discontent** policy to immediately locate violations.

Block data containing source code

Employees who are leaving the company might feel they have a right to the code they have written. You can take measures to protect it by defining the source code content type and setting up action rules that will fire if it is found.

You can protect your company's intellectual property by configuring your systems to block all source code leaving the network. You might customize the rule to recognize a specific source code type, then make sure the responsible party receives email notification of the action.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Open an existing policy and an appropriate rule, or create new ones.

3 Open the **Content** category and select **Content Type** | **is any of**, then click **?**

The **Content Type** pop-up menu appears.

4 Open the **Source Code** category and select one or more source code types.

If you don't know the source code type, select **Template** | **equals**, click **?** and select **Source Code** instead. The template covers a collection of common types.

5 Click **Apply**.

6 Click the **Action** tab.

The **Edit Action Rule** page appears.

7 Click **Add Action** and select an appropriate action rule. For example, if Security should receive notification, you might apply **Block** and **Assign to InfoSec** action rules.

8 Click **Save**.

Block transmission of financial data

Even the most dedicated employees might not realize the implications of failing to protect financial documents, or they might not know how to encrypt them.

You can protect financial data by adding a concept that finds a variety of financial documents to a rule, then attach an action rule to prevent them from leaving the network.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Open an existing policy and rule, or create new ones.

3 Open the **Content** category.

The **Edit Rule** page appears.

4 From the **Content** menu, select **Concept** | **is any of**, then click **?**.

The **Concept** pop-up menu appears.

5 Select the **Select All** checkboxes on financial concept categories, or open them and select specific document types.

You might select *BANK-STMT* from the *Banking and Financial Sector* category, or *CONFIDENTIAL* from the *Corporate Financial* category.

6 Click **Apply**.

7 Click the **Action** tab.

8 Click **+** and **Add Action**, then select the **Block and Notify Sender** action to protect the material and notify the sender of the violation.

9 Click **Save**.

Modify alphanumeric patterns in rules that produce false positives

If you are looking for personal identification numbers that violate privacy standards, but product part numbers that also match the pattern are being erroneously reported, you can define an exception that will eliminate those results.

The exception you create refines the rule to recognize only the patterns in the PINs so that only legitimate privacy violations are reported to the dashboard.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select an incident that reported a part number as a privacy violation.

3 In the **Group by** menu in the left pane, select **Rule**, then the privacy rule that produced the errors.

All incidents produced by that rule are listed.

4 Select the checkboxes of the false positive incidents.

5 Click **Tune Rule**.

The **Edit Rule** page appears with **Exceptions** selected. All of the parameters on the page are rule values that you can modify.

6 Type in text describing the exception in the **Notes** box, then redefine the parameters.

For example, if the part number has the same pattern as an identification number, but is preceded by "PN#", add a **Content** element that specifies **Keywords** | **contain none of** | **<PN#>**.

7 If there is no difference in the pattern, consider eliminating another element the incidents have in common.

For example, if all of the reported part number incidents come from the same department, create a **Source/Destination** element that specifies an email domain or **UserOrganization**.

8 Click **Save**.

After the rule runs, evaluate the incidents retrieved and make revisions if the results still do not meet your criteria.

Track intellectual property violations

Suppose you know that your company has lost intellectual property to a Chinese firm, and you suspect that the leak came from an insider in your Shanghai branch. You can create rule parameters that find the leaked documents and the suspected violator, then monitor his or her activities to build a legal case and prevent any more data loss.

Before you begin

You must have an Active Directory server and McAfee® Logon Collector connected to the McAfee DLP system.

You can track down the violation by identifying the information compromised, the recipient of the information, and the suspected user by creating rules with parameters that will pull related information from the directory server.

If you don't know the user's name, you can gradually develop his identity by searching for users in Shanghai, searching the user groups in your Engineering division, and identifying a sub-group that might contain the user. You might not know in advance what you might find, but you can use what you discover to ask the next logical question.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Open an existing policy, or create a new one.

3 From the **Actions** menu, select **Add Rule**.

The **Add Rule** page appears.

4 Type in a name and optional description.

5 Open the **Content** category and add content that describe the lost intellectual property.

For example, you might add keywords, an exact phrase found in the leaked documents, a file type, or a concept that will retrieve similar content.

6 Open the **Source/Destination** category and add a destination that might describe the recipients of the data.

For example, you might have an IP addresses, domains, or a geographic locations that will help to define the recipient.

7 Click **Save**.

8 After the rule retrieves incidents, click **Details** and examine the **Incident Details** page.

If a user ID or email address is reported, you can add that information to your rule so that you can monitor all of that user's transactions.

9 If you find significant results, add an action rule to the rule and redeploy it.

For example, you might block, quarantine, redirect, or notify an administrator of any new violations.

11 Rule elements

McAfee DLP rule elements provide granularity so you can create rules and policies best suited for your network environment.

Contents

- *Action rules*
- *Concepts*
- *Templates*
- *Content types*

Action rules

Action rules work by applying actions when rules generate incidents. Actions might be preventive, corrective, or protective, and the actions available depend on whether McAfee DLP Prevent or a proxy server is used to implement them.

When a rule produces an incident, use of an action rule can resolve problems in network traffic, trigger a remedial action in data repositories, or react to an action that has been taken at a network endpoint.

Differences between action and protection rules

McAfee DLP Endpoint protection rules are pre-configured with reactions to events that occur at endpoints. Because the design of endpoint and network McAfee DLP products differs, action and protection rules work in different ways.

- McAfee DLP network products allow action rules to have multiple actions that are attached to many different rules. Each of those rules can deploy the action once to network traffic, a repository, or endpoints.
- The McAfee DLP Endpoint product uses protection rules to apply reactions to many different endpoints that might be online (on-site) or offline (in contact with a domain controller) when a violation occurs.

How action rules work in different McAfee DLP products

Preventive, corrective, or protective actions are applied depending on whether they are used in **Data-in-Motion**, **Data-at-Rest**, or **Data-in-Use**.

- If preventive action is to be taken, action rules are applied to **Data-in-Motion**, which monitors email and webmail in network traffic. This feature requires configuration of an MTA (Mail Transport Server) or proxy server with McAfee DLP Prevent, which must be registered to McAfee DLP Manager.
- If corrective action is to be taken, action rules are applied to **Data-at-Rest**, which identifies data at risk in network repositories. This feature requires McAfee DLP Discover, which must be registered to McAfee DLP Manager.
- If protective action is to be taken, action rules are applied to **Data-in-Use**, which identifies problems at endpoints. This feature requires McAfee DLP Endpoint, which must be registered to McAfee DLP Manager.

If McAfee DLP Monitor and McAfee DLP Discover devices are both managed by McAfee DLP Manager, every rule can be configured to deploy one action of each of the three incident types.

How McAfee DLP Prevent uses action rules

Depending on whether McAfee DLP Prevent is configured with an MTA (Mail Transport Agent) or a proxy server, McAfee DLP Prevent can take up to eight different actions when a significant incident is detected.

McAfee DLP Prevent might use action rules to perform any of the following actions:

- Allow email that is determined to be legitimate.
- Block confidential data breaches.
- Bounce email that violates policies.
- Encrypt authorized transmissions.
- Monitor traffic and record incidents in a system log.
- Notify supervisory personnel of a violation.
- Quarantine suspicious traffic.
- Redirect messages that violate policy.

McAfee DLP Prevent can also capture network traffic for later forensic analysis, and block the transmission of sensitive data sent using specific protocols (for example, HTTP, SMTP, HTTP POST, etc.).

How McAfee DLP Endpoint uses action rules

Depending on what protection rules McAfee DLP Endpoint is configured to deploy, up to nine different online and offline actions can be applied when a significant event is detected.

McAfee DLP Endpoint might use action rules to perform any of the following actions:

- Block confidential data breaches.
- Delete email that violates policies.
- Encrypt authorized transmissions.
- Quarantine reported events.
- Request justification for blocked actions.
- Tag files.

- Monitor events.
- Notify users of violations.
- Store evidence of violations.

Online and Offline options

For each reaction provided by a protection rule, you must select an *Online*, *Offline* status, or both.

These terms refer to where a computer is located in relation to the internal network, so they might be considered "on-site" or "off-site".

Specifically, online/offline status is determined by whether or not the ePolicy Orchestrator IP address can be resolved with a DNS query. In other words, a user who is *offline* is not in contact with a network domain controller.

How McAfee DLP Discover uses action rules

Depending on the policies and rules deployed during a Discover scan, McAfee DLP Discover can take up to four different remedial actions when significant data is detected.

McAfee DLP Discover might use action rules to perform any of the following remedial actions:

- Copy a file at risk to another location.
- Move a file at risk to another location.
- Encrypt (password-protect) a file at risk.
- Delete a file at risk.

Each of these actions includes the ability to add the following actions:

- Notify users of violations found in scanned data.
- Record violations found in a system log.
- Assign incidents to one or more reviewers.
- Set a status that indicates the state of resolution.

Remediation can be pre-programmed by attaching an action rule to rules that produce incidents, or applied directly to incidents reported on the **Data-at-Rest** dashboard by clicking the **Remediation** button.

Add, modify, or delete action rules

Add actions to the list of standard action rules, modify existing ones, or delete them set up McAfee DLP Prevent to implement appropriate actions in response to specific policy violations.

Tasks

- *Add action rules* on page 112
  Add action rules to resolve problems when rules generate incidents.
- *Apply action rules* on page 113
  Apply action rules to rules monitoring data in motion, scanning data at rest, or identifying significant events on endpoints. When an incident is detected, the applied action rule is activated.
- *Assign responsibility for actions* on page 113
  Assign responsibility for actions by setting up action rules. For example, reviewers might be assigned to monitor results when incidents are found by a rule containing an action rule.
- *Change incident status with action rules* on page 113
  Change the status of incidents on the fly by defining action rules that are applied when they are found.
- *Clone action rules* on page 114
  Clone action rules to use the same actions in another rule.
- *Delete action rules* on page 114
  Delete action rules individually or in groups.
- *Modify action rules* on page 114
  Modify action rules to serve new purposes.
- *Log actions taken* on page 115
  If a syslog server has been configured to receive log entries, you can log actions to be taken when a rule hits.
- *Notify users of actions taken* on page 115
  Notify users of actions taken when incidents are found by setting up email notifications in action rules.
- *Reconfigure action rules for web content* on page 116
  You must reconfigure McAfee DLP Prevent action rules for use on proxy servers.
- *Remove actions from rules* on page 116
  Remove actions from rules without affecting other parameters of the rule.

Add action rules

Add action rules to resolve problems when rules generate incidents.

Some actions (for example, **Block** and **Encrypt**) are cannot be used in the same action rule. If you select incompatible actions, an error message appears when you attempt to save your changes.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 From the **Data-in-Motion**, **Data-at-Rest**, or **Data-in-Use Actions** menus, select **Add Action Rule**.

The three categories determine where the actions will be implemented — on the network, in a repository, or on an endpoint.

3 Type in a name and optional description.

4 From the **Actions** categories, select the components of the action rule.

Selection of components in **Data-at-Rest** or **Data-in-Use** action rules determines whether or not additional information is needed.

5 Click **Save**.

Apply action rules

Apply action rules to rules monitoring data in motion, scanning data at rest, or identifying significant events on endpoints. When an incident is detected, the applied action rule is activated.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Select the action rule to be applied.

- For **Data-in-Motion**, open the **Prevent Action** category and select an action from the list.
- For **Data-at-Rest**, open the **Remediation Policy** category and select an action from the list.
- For **Data-in-Use**, open the **Data-in-Use Policy** category and select one or more actions.

3 Click **Save**.

Assign responsibility for actions

Assign responsibility for actions by setting up action rules. For example, reviewers might be assigned to monitor results when incidents are found by a rule containing an action rule.

The **Incident Reviewer** parameter applies to **Data-in-Motion** and **Data-at-Rest** action rules. It cannot be used to react to **Data-in-Use** events.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Click a rule.

The **Edit Action Rule** page launches.

3 From the **Incident Reviewer** menu, select a group or user.

The existing groups and users are displayed.

4 Click **Save**.

Change incident status with action rules

Change the status of incidents on the fly by defining action rules that are applied when they are found.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Open an action rule.

The **Edit Action Rule** page appears.

3 From the **Incident Status** menu, select a status.

4 Click **Save**.

The status is applied to data found by the rule to which the action rule is appended.

Clone action rules

Clone action rules to use the same actions in another rule.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Open an action rule.

The **Edit Action Rule** page appears.

3 In the **Action Rule Name** field, enter a new name.

4 Click **Save**.

The **Action Rules** page displays the new action rule.

Delete action rules

Delete action rules individually or in groups.

Action rules that have been applied to rules are in use and cannot be removed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Select the action rules to be deleted.

3 Delete action rules in one of two ways.

- From the **Actions** menu, select **Delete**.
- In the **Delete** column, click the trash can icon of the rule to be deleted.

Modify action rules

Modify action rules to serve new purposes.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Open the action rule to be modified.

3 Open the **Actions** components and edit the parameters.

4 Click **Save**.

Log actions taken

If a syslog server has been configured to receive log entries, you can log actions to be taken when a rule hits.

The **Syslog Notification** parameter applies to **Data-in-Motion** and **Data-at-Rest** action rules. It cannot be used for **Data-in-Use** events.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Click the action rule to be modified.

3 Open the **Syslog Notification** category.

4 Select **Enable**.

5 Click **Save**.

Notify users of actions taken

Notify users of actions taken when incidents are found by setting up email notifications in action rules.

For example, users who are tasked with monitoring results might be automatically informed of developments for incidents that are collected in cases.

The **Email Notification** parameter applies to **Data-in-Motion** and **Data-at-Rest** action rules. It cannot be used for **Data-in-Use** events.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Click an action rule, or create a new one.

3 On the **Edit Action Rule** page, open the **Email Notification** component.

4 Type a valid email address into the **From** field.

Email addresses are invalid if they include special characters (for example, &, *, %), but if valid addresses are also included, notification will still be sent to those users.

5 Type one or more addresses into the **To** and **Cc** fields.

6 (Optional) Select checkboxes to notify managers, reviewers, senders, or recipients.

The options available depend on the McAfee DLP appliance. Managers can be identified only if an Active Directory server has been added, but other categories are user-defined. Reviewer is the only option available on McAfee DLP Discover.

7 (Optional) Type in a **Subject** and **Message**.

These fields accept dynamic variables, enabling you to set up automatic responses to routine situations. They an be used to alert users to details of the violation automatically (for example, `## Filename found by the ##Rule violated the ##Policy`).

8 Click **Save**.

Reconfigure action rules for web content

You must reconfigure McAfee DLP Prevent action rules for use on proxy servers.

McAfee DLP Prevent supports BOUNCE, ENCRYPT, MONITOR, NOTIFY, QUARANTINE or REDIRECT actions, but proxy servers can only ALLOW or BLOCK web content.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 Click the action rule to be reconfigured.

3 Type in a new name and optional description.

4 Click **Save As** to create a copy of the action rule.

The new rule appears on the **Action Rules** page.

5 Open the new action rule.

6 On the **Edit Action Rule** page, open the **Prevent Action** component and select an ALLOW or BLOCK action from the menu.

7 Click **Save**.

The new rule appears on the **Action Rules** page.

Remove actions from rules

Remove actions from rules without affecting other parameters of the rule.

This task removes only actions that have been applied to rules, not the rules themselves. Action rules that have been applied to rules in use cannot be removed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click the **Policy Name**, then the **Rule** that contains the action that is to be removed.

3 On the **Edit Rule** page, select the **Actions** tab.

4 On the list of actions, locate the action to be removed.

5 Click the **X** in the right column.

If you cannot see the column, expand your dashboard.

6 Click **Save**.

Concepts

McAfee DLP uses content and session concepts to match patterns in traffic on the application or session layers. Content concepts are used to find data in motion or at rest, and session concepts are used to recognize content found in data being exchanged between clients and servers.

Types of concepts

Two concept types are used to find related patterns of data in network traffic or data repositories.

- *Content concepts* contain text patterns and regular expressions to match patterns to data on the **Application** layer (Layer 7).
- *Session concepts* target exchanges of data between applications on the **Session** layer (Layer 5). They can be used to recognize content found in multiple objects contained in a single flow.

How content concepts work

Content concepts contain related patterns of data that can be matched to data in motion or at rest. They find collections of significant data related to a single issue in application data.

Most of the concepts that are shipped with your McAfee DLP appliances are listed under the **User-Defined** tab. Only a few **Built-in** concepts are constructed with proprietary algorithms. For example, a content concept can be used to collect credit card numbering patterns that can be matched to network data. You might use one of the factory default concepts (AMEX, CCN, DISCOVER, MASTERCARD) to find standard payment card violations quickly, or you can add one that focuses only on patterns used by retail cards.

If you are an advanced user, you can construct session concepts to identify data that is being exchanged between clients and servers, or to find multiple objects in a single flow (for example, email and attachments).

Regular expression syntax for concepts

Regular expressions are used to build McAfee DLP concepts. Unlike those used by McAfee DLP Endpoint, they do not use POSIX syntax.

Table 11-1 Supported regular expressions

Expression	Definition
\n	line feed
\r	carriage return
\f	form feed
\b	backspace
\a	bell
\t	tab
\k	disables Perl/POSIX set range restrictions
\K	enables Perl/POSIX set range restrictions

Table 11-1 Supported regular expressions *(continued)*

Expression	Definition
\0xN	the hex ascii character equivalent to N
\nnn	the octal character of value nnn
\d	digit 0-9
\D	not digit 0-9
\c	any alpha A-Z or a-z
\C	not any alpha A-Z or a-z
\w	any alphanumeric \c or \d
\W	not alphanumeric ^\w
\s	any space [\ < > ; \f \n \r \t \[\]]
\S	not any space ^\s
\p	any space or field delimiter [\ -\\ :-@\[-`{-~ \[\]]
\P	not any space or field delimiter ^\p
\i	case sensitivity off
\I	case sensitivity on
[...]	character sets, for example, [3-6a-c] = 3,4,5,6,a,b,c
x-y	character ranges T-X = T,U,V,W,X
^	invert, for example, ^\0x0 are all characters except NULL
\	literal backslash (transforms metacharacters into ordinary characters). Examples: \\ \. \& \[\] \<space> * \+

Add, apply, restore, and delete concepts

Concepts must be maintained to match changing data patterns and session content. In addition to the standard concept parameters, you can set conditions to matches based on extraneous factors, or use them to extend rules.

Tasks

- *Add content concepts* on page 119

  Add content concepts to match text patterns and regular expressions to data in traffic or repositories.
- *Set conditions for matching concepts* on page 120

  Set limitations on concepts that instruct the system to report matches only if certain conditions are met.
- *Add session concepts* on page 121

  Add session concepts to inspect all communications between two parties when a pattern is matched. Because the session layer is monitored, you will be able to find multiple objects contained in a single flow (for example, an email attachment as well as the mail body).
- *Apply concepts to rules* on page 122

  Apply content concepts to rule definitions to match patterns in data traffic or repositories.
- *Restore user-defined concepts* on page 122

  Restore the **User-Defined** concepts to their original state if they have become corrupted or difficult to handle.
- *Delete custom concepts* on page 122

  Delete custom concepts from the **Concepts** page if they are no longer useful.

Add content concepts

Add content concepts to match text patterns and regular expressions to data in traffic or repositories.

When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, _). You can add up to 512 content and session concepts to match patterns in network and repository data.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Concepts**.
- On your McAfee DLP appliance, select **Policies** | **Concepts**.

2 Click **Add Concept**.

3 Type in a name (uppercase only) and an optional description.

4 Click **?** to file the concept under a category.

All concepts in a category can be used in queries and rules.

5 If one of the available algorithms matches the aim of the new concept, you can select it from the **Algorithm** menu to fine-tune the pattern match.

An expression might match a pattern correctly, but its granularity might not be fine enough to eliminate imprecise results. Adding an algorithm to the definition evaluates the pattern arithmetically to ensure a perfect match.

For example, U.S. Social Security and credit numbers might be 9 or 16 digits, but each digit has a significance beyond the pattern. Social Security numbering signifies the date and birthplace of the cardholder, while some credit card digits identify the issuer (such as MasterCard or Visa). The algorithm mathematically verifies authenticity of these additional characteristics in addition to the numbering patterns.

6 If you want to upload a list of existing expressions or patterns, click **Browse** and select the file.

7 Click **Import Expressions** to load expressions from a file, or enter expressions in the **Expression** field.

The size of the imported file cannot exceed 10K.

Escape all metacharacters to ensure literal interpretation (for example, `www\.deadspin\.com`).

8 If you want to edit the list of expressions, or just keep a copy, click **Export Expressions** to save them to your desktop. You can debug them in a text editor, then reimport.

9 If you don't have a document to upload, or want to use text and regular expressions to build a new concept, enter a value in the **Expression 0**: field. Click **+** to add an expression, and repeat until all expressions are added.

10 Click **Validate**, then enter a sample string. If it matches, go on to the next step. The **Matches String** returns a true or false acknowledgement.

11 Use one of the concept conditions (**Count**, **Percentage Match**, **Number of lines/bytes**, **Proximity**) to modify the action of the concept.

Concept conditions narrow the match to specific circumstances. For example, if you want the system to wait until the concept patterns are found three times before being reported to the dashboard, select **greater than** from the **Condition** menu, and enter `3` in the value field.

12 Click **Save**.

When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, `hello\_world`). Other metacharacters and ASCII characters (such as `&#x0020`, `&#x0009`, `&#x000C`, and `&#x200B` for space, tab, form feed, and zero-width space) can also be used to define concept expressions.

Set conditions for matching concepts

Set limitations on concepts that instruct the system to report matches only if certain conditions are met.

Before you begin

The concept to which conditions are to be added should be retrieving predictable results.

Only **User-Defined** or custom concepts accept conditions.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Concepts**.
- On your McAfee DLP appliance, select **Policies** | **Concepts**.

2 Open a concept category and click a **Concept Name**.

3 On the **Edit Concept** page, define one or more concept conditions to modify the circumstances under which a match is reported.

- **Count** — Incidents are not reported unless the expression is found at least, or more than a specific number of times.
- **Percentage** — Incidents are not reported unless the expressions are found within a percentage of the text in a file. For example, if less than 50 percent is configured, the concept is a match if the patterns exist within the first 50 percent of the text in the file — but in a 3 MB file, only 4 KB might be text, so the match would have to be found within the first 2 KB. Alternatively, if the setting is greater than 75 percent, then the match would occur only if the pattern was found toward the end of the file (3 to 4 KB).
- **Number of lines from beginning** — Incidents must not be reported unless the expression is found in a specified range of lines from the beginning of the file.
- **Number of bytes from beginning** — Incidents must not be reported unless the expression is found in a specified number of bytes from the beginning of the file.
- **Proximity** — Incidents must not be reported unless the expression is found at a numeric byte location.

4 Click **Save**.

Add session concepts

Add session concepts to inspect all communications between two parties when a pattern is matched. Because the session layer is monitored, you will be able to find multiple objects contained in a single flow (for example, an email attachment as well as the mail body).

When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, `\_`).

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Concepts**.
- On your McAfee DLP appliance, select **Policies** | **Concepts**.

2 Click **Add Concept**.

3 In the **Advanced** category, select the **Session Type** option.

4 Type in a name (uppercase only) and optional description.

5 Select an algorithm to ensure self-correction of incorrectly entered parameters.

For example, if you create a MasterCard expression that uses an incorrect numbering sequence, the algorithm will ignore the pattern and replace it with the correct sequence.

6 Click **?** to file the concept under a category.

All concepts in a category can be used in queries and rules.

7 If you want to upload a list of existing expressions or patterns, click **Browse** and select the file.

8 Click **Import Expressions** to load expressions from a file, or enter expressions in the **Expression** field.

Escape all metacharacters to ensure literal interpretation (for example, `www\.deadspin\.com`).

9 If you want to edit the list of expressions, or just keep a copy, click **Export Expressions** to save them to your desktop. You can debug them in a text editor, then reimport.

10 If you don't have a document to upload, or want to use text and regular expressions to build a new concept, enter a value in the **Expression 0**: field. Click **+** to add an expression, and repeat until all expressions are added.

11 Click **Validate**, then enter a sample string. If it matches, go on to the next step. The **Matches String** returns a true or false acknowledgement.

12 Use one of the concept conditions (**Count**, **Percentage Match**, **Number of lines/bytes**, **Proximity**) to modify the action of the concept.

Concept conditions narrow the match to specific circumstances. For example, if you want the system to wait until the concept conditions are found three times before being reported to the dashboard, select **greater than** from the **Condition** menu, and enter `3` in the value field.

13 Click **Save**.

When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, `hello\_world`). Other metacharacters and ASCII characters (such as `&#x0020`, `&#x0009`, `&#x000C`, and `&#x200B` for space, tab, form feed, and zero-width space) can also be used to define concept expressions.

Apply concepts to rules

Apply content concepts to rule definitions to match patterns in data traffic or repositories.

The rule definition might contain many parameters, one of which might be a pattern defined in a concept. For example, the HATE-RACISM concept might be paired with a user group and a document type to find evidence of specific suspected violations.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
   - On your McAfee DLP appliance, select **Policies**.

2 Open a policy, then a rule.

   The **Edit Rule** page appears.

3 Open the **Content** category.

4 Select **Concept** | **is any of** and click **?**.

5 From the **Concept** menu, open a category and select one or more patterns.

6 Add one or more conditions to set limitations on incident reporting.

7 Click **Save**.

8 Wait for the rule to run, then select **Incidents** to view the result.

Restore user-defined concepts

Restore the **User-Defined** concepts to their original state if they have become corrupted or difficult to handle.

Only the original list of concepts under the **User-Defined** tab can be restored. Concepts listed under the **Built-in** tab cannot be edited, so they need not be restored.

Custom concepts cannot be recovered.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Concepts**.
   - On your McAfee DLP appliance, select **Policies** | **Concepts**.

2 Open a category and select one or more concepts.

3 Select **Actions** | **Restore Default**.

Delete custom concepts

Delete custom concepts from the **Concepts** page if they are no longer useful.

You cannot delete **User-Defined** or **Built-In** concepts.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Concepts**.
   - On your McAfee DLP appliance, select **Policies** | **Concepts**.

2 Open the category containing the custom concepts.

3 Select the concepts to be deleted.

- From the **Actions** menu, select **Delete**.
- In the **Delete** column, click the trash can icon of the concept to be deleted.

Typical scenarios

McAfee DLP content concepts are useful for performing routine monitoring tasks. This section discusses two typical scenarios and provides the high-level steps for each.

Identify Human Resources violations

Employees who have legitimate complaints about managers or coworkers might not feel that it is safe to come forward, and you might have to develop the case by getting concrete evidence of violations.

If you suspect such a situation, you can configure a customized concept that monitors internal communications to find and stop Human Resources violations before they damage employee relationships or morale. For example, you might edit the standard HATE-RACISM concept to include unacceptable language you've heard in the workplace, create a policy and add it to a rule that monitors chat and email transmissions, and let it run to verify its efficacy.

You might also add an action rule to automatically assign any incidents found to the legal team.

You might have to wait for some time to allow the capture engine to index new data so the new concept pattern can be matched to the developing data stream. The amount of time you must wait depends on the time frame in which you might expect to find the pattern. For example, if you suspect that violations are occurring regularly, you might wait a few hours or a day. If not, you might check the incidents dashboard for results on a daily or weekly basis.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **DLP Policies** | **Concepts**.
- On your McAfee DLP appliance, select **Policies** | **Concepts**.

2 Open the *Acceptable Use* concepts category and click HATE-RACISM.

The **Edit Concept** page appears.

3 In the **Content** category, add, delete, or modify the expressions to fit the circumstances, then **Save**.

4 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

5 From the **Actions** menu, select **Add Policy**, and add a name and optional description.

6 Select one or more **Suppress incidents** checkboxes.

7 From the **Actions** menu, select **Add Rule**, and add a name and optional description.

8 Open the **Content** category and select **Concept > is any of**.

9 Click **?** and select the HATE-RACISM checkbox from the **Acceptable Use** concept category.

10 Click **Apply**, then **Save** the rule and the policy.

11 Let the rule run. After some time, reopen the policy and monitor matches using the **Chart** feature.

12 When you see that useful results are being generated as expected, restore reporting to the dashboards by clearing the checkboxes and **Save**.

13 On the **Incidents** dashboard, monitor results by periodically checking your new policy in the **Group by...** frame.

Monitor social networking traffic

Using McAfee DLP standard content concepts to find patterns in traffic is one way to monitor and manage usage of social networking sites.

For example, employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked in the process. You might use the BLOGPOST concept to identify traffic to and from such sites.

On the **Concepts** page, open the **Online** category and click BLOGPOST to find out what sites are covered. If necessary, modify the concept to include additional sites so that you can figure out how to control the situation.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Concept** | **is any of** and click **?**.

The **Concept** pop-up menu opens.

4 From the **Online** category, select the BLOGPOST checkbox.

5 Click **Apply**.

6 Click **Search** or **Save as Rule**.

Templates

Templates are collections of components that eliminate the need to perform routine operations repetitively. They can be used to consolidate multiple queries, capture filter parameters, and rule definitions into a single entity.

Standard templates are designed to serve a wide variety of business operations, and customized templates are used for a single purpose. Custom templates are especially useful for streamlining the process of rule-tuning.

How templates are used

You might use a template to create a name for a range of IP or email addresses so you can refer to them as a group. You might even use a template to enable all of the endpoint protection rules, then add them to a rule that protects all data in use on a defined network path.

Templates are designed to use the same organizational principles as rules, capture filters, and searches. Learn to construct a custom template by looking at the standard ones listed on the **Templates** page.

How templates work

Using templates saves time when searching, creating rules, or building capture filters. They make entering the same values multiple times unnecessary.

Pre-installed standard templates can be used as tools to help find groups of related elements in network data.

> For example, the Source Code template contains patterns for most of the source code file types. It might be used to monitor network data for proprietary programs that insiders are attempting to send outside of the company.

Review template construction

Review template construction to see how templates mirror the construction of searches, rules, and capture filters. Because they share a common structure, templates can be used to abbreviate all of those operations.

Each component type on the templates, rules, search and capture filter including templates that are related to the category.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Templates**.
- On your McAfee DLP appliance, select **Policies** | **Templates**.

2 Click any **Template Name** on the page.

Use the same procedure for standard or custom templates.

3 Open **Construction**.

4 Review the parameters by examining the value field, or by clicking the **?** icon.

Extending queries or rules with templates

Each component menu includes a **Template** selection that can be used with any component to provide a wide-ranging qualifier for a search or rule.

When used as an additional parameter to extend any other component selection, a template can be used to extend a query or rule. For example, if a query uses a keyword or concept component to find any file containing confidential content, it can be extended to specific document types by using an **Office Document** template.

> A CONFIDENTIAL concept might be used in a template to match data containing common words and phrases found in proprietary data. A template could be added to limit that search to office documents or email message bodies.

Add, modify, and delete templates

Managing templates will help you to use them to best advantage. You can add, modify, or delete them, or remove those that are no longer useful from rules or filters.

Tasks

- *Add or modify templates* on page 126
  Add or modify templates that define collections of content types, ports, protocols, email or IP addresses, user groups, endpoints, registered data, and other related data entities.
- *Delete templates* on page 126
  Delete templates that are no longer useful. They can be deleted individually or as groups.
- *Remove templates from rules* on page 127
  Remove templates that have been applied to rules or capture filters.

Add or modify templates

Add or modify templates that define collections of content types, ports, protocols, email or IP addresses, user groups, endpoints, registered data, and other related data entities.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Templates**.
   - On your McAfee DLP appliance, select **Policies** | **Templates**.
2 Select **Actions** | **Add Template**.
3 Enter a name and optional description.
4 Select a **Component Type**.

   Compare this menu with the categories on the **Advanced Search** or **Edit Rules** pages.

5 Open the **Construction** category.
6 From the menus, select a parameter type, a condition, and enter a value in one of two ways.
   - Click **?**, select parameters from the pop-up menu, and **Apply**.

     In some cases, **?** will launch a context-sensitive help topic.
   - Type a value into the value field.

   If no pop-up menu is available, a text entry is required.
7 Click **Save**.

Delete templates

Delete templates that are no longer useful. They can be deleted individually or as groups.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Templates**.
   - On your McAfee DLP appliance, select **Policies** | **Templates**.
2 Select the templates to be deleted.

3 Delete templates in one of two ways.
   - From the **Actions** menu, select **Delete**.
   - In the **Delete** column, click the trash can icon of the template to be deleted.

Remove templates from rules

Remove templates that have been applied to rules or capture filters.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Policies**.
   - On your McAfee DLP appliance, select **Policies**.
2 Select a policy containing a rule to which a template has been applied, then select the rule.

   The **Edit Policy** page appears.
3 Click **-** to remove the element containing the template.
4 Click **Save**.

Typical scenarios

Use the following scenario to get a general understanding of how templates can be used in searches, rules, and capture filters.

Monitor source code using a template

The source code template contains most of the source code file types, so unless proprietary code is involved, it can be tracked. If you have to keep source code secure, you can add a template parameter to a rule definition to keep it from leaving the intranet.

Pair the source code template with FTP and email protocols, and then add an action rule to notify an information security administrator if an attempt is made to transmit it to a location outside of the intranet.

Find images using a template

Find images using templates to expedite searching of large graphics caches. The different image types included can retrieve image data in any format.

Add a **Thumbnail Match** column to your dashboard to scan results quickly. Avoid timeouts caused by retrieving large image files by adding additional search terms.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Content** category.
3 Select **Template** and click **?**.

   The **Template** pop-up menu opens.

4 Select the **Common Image Files** template.

5 Click **Search** or **Save as Rule**.

Use a template to protect archives

You can use a standard or customized template in a rule to monitor and manage archives on a regular basis.

For example, you might want to add the **Archive Formats** template to a rule that keeps compressed files from being emailed to China.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy, then a rule.

The **Edit Policy** window appears.

3 From the **Content** category, select **Template** | **is any of** and click **?**.

The **Template** pop-up menu opens.

4 From the **Template** menu, select **Archive Formats** and click **Apply**.

5 From the **Source/Destination** category, select **GeoIP Location** | **is any of** and click **?**.

The **GeoIP Location** pop-up menu opens.

6 From the **GeoIP Location** menu, select **Asia Pacific**, select the *China* checkbox, and click **Apply**.

7 Click **Actions**, then **Add Actions**.

8 From the **Actions** menu, select **Bounce and Notify Sender**.

You might want to click **Action Rules** and delete the sender notification from the rule, or create a new one.

9 Click **Save**.

Use a template to search for documents

You can use a template to search for documents that are owned by specific users.

Before you begin

To provide a path to user accounts, an LDAP server must be added to McAfee DLP Manager.

For example, you might want to find all Microsoft Office documents belonging to a user. The **Office Application Files** template identifies files that are created by Microsoft applications, plus files CSV and PDF formats.

If you don't know what the template does, open it from the **Templates** page to examine its construction. You might want to edit it, or use it to create a template that contains only Microsoft Word and Excel file formats.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Template** | **is any of** and click **?**.

The **Template** pop-up menu opens.

4 From the Template menu, select **Office Application Files**.

5 Open the **Source/Destination** category.

6 From the component menu, select **User Name** | **is any of** , click **?**, and select the directory server.

The **AD pop-up** window appears.

7 Click **Find**, select the user, and click **Apply**.

8 Click **Search**.

The **Search Results** window appears.

Content types

The McAfee DLP classification engine recognizes a variety of content types — such as applications, documents, and network protocols — that you can specify in your rules.

Advanced documents content types

The following Advanced document content types are supported by the capture engine.

Table 11-2 Advanced document content types

Content type	Description
BDB	Blaise Database
DBM	DataBoss Menu (Cold Fusion Template)
FrameMaker	Adobe FrameMaker
PS	Adobe Postscript
SQL	MySQL or MS SQL
CSS	Cascading Style Sheets
DBX	Database Index (Outlook Express)
HTML	Hypertext Markup Language
Quicken	Quicken (Intuit)
Stockdata	Stockdata
DBF	Database File (DBASE)
EPS	Encapsulated PostScript (Adobe)
Lotus	Lotus Notes (IBM)

Table 11-2 Advanced document content types *(continued)*

Content type	Description
RichText	RichText (Microsoft)
XML	Extensible Markup Language

Apple application content types

The following Apple application content types are supported by the capture engine.

Table 11-3 Apple application content types

Content type	Description
AppleWorks	AppleWorks
WN	Amiga WriteNow
MCW	Macintosh MacWrite
vCalendar	Internet Mail Consortium calendar

Binary content types

The following binary content types are supported by the capture engine.

Table 11-4 Binary content types

Content type	Description
Binary	Binary
LIF	Logical Interchange Format
SKR	PGP private keyring file

Chat content types

The following chat content types are supported by the capture engine.

Table 11-5 Chat content types

Content type	Description
AOL_Chat	America Online chat
MSN Chat	Microsoft Network chat
Yahoo_Chat	Yahoo chat

Compressed and archive formats

The following compressed and archive formats are supported by the capture engine.

Table 11-6 Compressed and archive formats

Content type	Description
BinHex	Binary-to-hexidecimal
GZIP	GNU zip
StuffIt	Stuffit
ZIP	ZIP
Compress	Compress
MS Cabinet	Microsoft Cabinet

Table 11-6 Compressed and archive formats *(continued)*

Content type	Description
TAR	Tape archive
EncryptedZip	Encrypted Zip
RAR	Roshal Archive
TNEF	Transport Neutral Encapsulation Format

Desktop content types

The following desktop content types are supported by the capture engine.

Table 11-7 Desktop content types

Content type	Description
ACursor	
Cursor	
Icon	

Engineering drawing and design content types

The following engineering drawing and design content types are supported by the capture engine.

Table 11-8 Engineering drawing and design content types

Content type	Description
AccelPCad	Accel P-CAD
BSDL	Boundary Scan Description Language
FreeHand	Adobe FreeHand
Mathematica	Wolfram Mathematica
PhotoShop	Adobe PhotoShop
TangoPCad	Tango P-CAD
Visio	Microsoft Visio
AllegroPCB	Cadence Allegro PDB Designer
CatiaCad	Computer-aided 3D Interactive Application
Gerber	Gerber CAD
Matlab	Matrix Laboratory
SolidWorks	SolidWorks Toolbox
UnigraphicsCad	Unigraphics CAD
VisualCad	Visual CADD
AutoCad	Autodesk AutoCAD
CSF	Custom Statement Formatter CAD
MathCad	Mathcad
PageMaker	Adobe PageMaker
Spice	Simulation Program Integrated Circuits Especially
ViewLogic	Viewlogic

Executable content types

The following executable content types are supported by the capture engine.

Table 11-9 Executable content types

Content type	Description
ELF	Executable and linking format
IBMApp	IBM applications
MacApp	Macintosh applications

Image content types

The following image types are supported by the capture engine.

Table 11-10 Image content types

Content type	Description
BMP	Bitmap
JPEG	Joint Photographic Experts Group
MacPaint	Macintosh MacPaint
PICT	Apple Macintosh Picture format
SuperPaint	Aldus Macintosh SuperPaint
GIF	CompuServe Graphics Interchange Format
MSMetaFile	Microsoft Metafile
PAL	Pearson Asset Library
PNG	Portable Network Graphics
TIFF	Tag Image File Format
IFF	Image File Format
MacDraw	Apple Macintosh MacDraw
PCX	Corel Paintbrush
RDIB	Device-independent bitmap file

Language classification content types

The following content types are used by the capture engine to sort non-English data into categories.

Table 11-11 Language classification content types

Content type
Arabic
Chinese (simplified)
Chinese (traditional)
Dutch
English
French
German
Greek
Hebrew

Table 11-11 Language classification content types *(continued)*

Content type
Italian
Japanese
Korean
Polish
Portuguese
Spanish
Russian
Turkish
Vietnamese

Mail content types

The following mail content types are supported by the capture engine.

Table 11-12 Mail content types

Content types	Description
Eudora	Qualcomm Eudora
MIME	Multipurpose Internet Mail Extensions
Mail_Header	Mail header
SMTP	Simple Mail Transfer Protocol
Flow_Header	Flow header
MSExchange	Microsoft Exchange
POP3	Post Office Protocol 23
WebMail	Webmail
IMAP	Internet Message Access Protocol
MSOutlook	Microsoft Outlook
RFC822	Internet email standard

Microsoft content types

The following Microsoft content types are supported by the capture engine.

Table 11-13 Microsoft content types

Content type	Description
MSMoney	Microsoft Money
MSWrite	Microsoft Write
MSPassword	Microsoft Password
MSRegistry	Microsoft Registry

Multimedia content types

The following multimedia content types are supported by the capture engine.

Table 11-14 Multimedia content types

Content type	Description
AIFF	Audio Interchange File Format
ICY	I Can Yell (SHOUTcast streaming protocol)
MP3	Moving Picture Experts Group 3 (audio compression)
Movie_ANI	South Asia Multimedia News Agency
RCP	Rich Client Platform
RTSP	Real Time Streaming Protocol
Shockwave	Adobe Shockwave
ASF	Advanced Streaming Format
MIDI	Musical Instrument Digital Interface
MPEG	Moving Picture Experts Group (audio/video compression)
NIFF	Notation Interchange File Format
RIFF	Resource Interchange File Format
RealMedia	RealMedia
SoundFont	SoundFont
AVI	Audio Video Interleave
MIDI_RMI	Musical Instrument Digital Interface in RIFF format (Microsoft)
MPlayer	The Movie Player
QuickTime	Apple QuickTime Player
RMMP	RIFF Multimedia Movie File Format
SD2	Sound Designer 2
WAVE	Microsoft Wave

Office application content types

The following office application content types are supported by the capture engine.

Table 11-15 Office application content types

Content type	Description
CSV	Comma-separated values
EncryptedPowerpoint	Encrypted Microsoft PowerPoint
MSProject	Microsoft Project
OpenOfficeSpreadsheet	Open Office Spreadsheet
Powerpoint	Microsoft PowerPoint
EncryptedExcel	Encrypted Microsoft Excel
EncryptedWord	Encrypted Microsoft Word
MS Word	Microsoft Word
OpenOfficeText	Open Office text
WordPerfect	Corel WordPerfect

Table 11-15 Office application content types *(continued)*

Content type	Description
EncryptedPDF	Encrypted Adobe Portable Document Format
Excel	Microsoft Excel
OpenOfficePresentation	Open Office presentation
PDF	Adobe Portable Document Format

Peer-to-peer content types

The following peer-to-peer content types are supported by the capture engine.

Table 11-16 Peer-to-peer content types

Content type	Description
BitTorrent	BitTorrent
Kazaa	Kazaa
WinMX	Windows Peer Network Protocol
DirectConnect	DirectConnect
MP2P	Mobile peer-to-peer
eDonkey	eDonkey
Gnutella	Gnutella
Sherlock	Sherlock
eMule	eMule

Protocol content types

The following protocols are supported by the capture engine.

Table 11-17 Protocol types

Content type	Protocol
CITRIX	Citrix
FTP	File Transfer Protocol
FTP_Response	File Transfer Protocol Response
HTTP_Header	Hypertext Transfer Protocol header
HTTPS	Secure Hypertext Transfer Protocol
HTTP_Redirect	Hypertext Transfer Protocol redirect
HTTP_Error	Hypertext Transfer Protocol error
IMAP	Internet Message Access Protocol
PCAnywhere	Symantec PCAnywhere
RPC	Remote Procedure Call
SSH	Secure Shell
VNC	Virtual Network Computing
Crypto	Cryptographic protocol
IRC	Internet Relay Chat
POP3	Post Office Protocol 3

Table 11-17 Protocol types *(continued)*

Content type	Protocol
SMB	Server Message Block
Skype	Skype
ICQ	Internet Control Questionnaire
LDAP	Lightweight Directory Access Protocol
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol
Telnet	Telnet

Source code content types

The following source code content types are supported by the capture engine.

Table 11-18 UNIX content types

Content type	Description
Ada_Source	Ada language
Basic_Source	Beginner's All--purpose Symbolic Instruction Code
Cobol_Source	Common Business-Oriented Language
Java_Source	Java language
Perl_Source	Practical Extraction and Reporting Language
Think_Pascal	Think Pascal (Apple) language
XQuery_Source	XML query language
Assembly_Source	Assembly language
C++_Source	C++ language
FORTRAN_Source	IBM Mathematical Formula Translating System language
Lisp_Source	Location/Identifier Separation Protocol language
Python_Source	Python language
VHDL_Source	Verilog Hardware Description Language
BREW	Binary Runtime Environment for Wireless
C_Source	C language
JavaScript	JavaScript language
Pascal_Source	Pascal language
Think_C	Think C (Apple) language
Verilog_Source	Verilog hardware definition language

Unclassified content types

The following other content types are supported by the capture engine.

Table 11-19 Other content types

Content types	Description
ASCII	American Standard Code for Information Interchange
CVS	Concurrent Versions System

Table 11-19 Other content types *(continued)*

Content types	Description
CAP	Packet Capture
PCAP	Packet Capture
CMS	Content Management System
iGaming	iGaming

UNIX content types

The following UNIX content types are supported by the capture engine.

Table 11-20 UNIX content types

Content type	Description
Bourne_Shell	Bourne shell
BASH_Shell	Bourne-again shell
C_Shell	C shell
K_Shell	Korn shell

12 Policy configuration options

The McAfee DLP user interface contains several areas where you can configure policies and rules. Some configuration options apply to a specific McAfee DLP product.

Contents

- *Policy definition options*
- *Rule options*
- *Action rule options*
- *Template options*
- *Concept options*
- *Document property options*
- *Registered document options*
- *Policy setting options*

Policy definition options

Basic policy definitions determine if the policy is active, which devices to apply the policy to, and the users who can access the policy.

Table 12-1 Policy definition options

Option	Definition
Policy Name	Unique name for the policy (required). Policy names must use only alphanumeric characters. Non-alphanumeric characters might generate an error message.
Policy Description	Optional description.
Owner	A group whose members can access the policy. If you are logged on as a member of one of the default groups, only that group is displayed, and other options are not available.
State	Policies can only have one of two states: active or inactive. The default is inactive. New policies are inactive by default to allow users to build a customized system. Using only the policies that meet their objectives optimizes performance and makes the most efficient use of the McAfee DLP system.
Region	Policies usually belong to a group that is defined by a region. The default region is North America.
Suppress incidents	Suppress incidents to keep them from being reported to dashboards while rules are being tuned or while troubleshooting. Selecting **Data-in-Motion** suppresses all incidents found in moving network traffic. Selecting **Data-at-Rest** suppresses all incidents found in static file or database repositories. There is no suppression option available for **Data-in-Use** events.
Devices	Specifies the devices the policy is applied to. The **None** checkbox is used for policies that are not yet deployed. Selecting the **Host** checkbox creates a policy that will be deployed to the host when an endpoint is registered.

Rule options

Rules contain conditions configured on three tabs.

- The **Define** tab contains parameters to match inspected data.
- The **Actions** tab specifies the action to take on matching data.
- The **Exceptions** tab specifies exceptions for the rule. Up to eight exceptions can be specified using all of the parameters available on the **Define** tab, except for **Endpoint** and **Date/Time**.

Table 12-2 Rule parameter options

Option	Definition	Applicable products
Content	Defines patterns of data with keywords, concepts, content types, or templates.	Any
Source/Destination	Specifies a source or destination IP address, email address, URL or Active Directory information.	• McAfee DLP Monitor • McAfee DLP Prevent
File Information	Defines files according to size, signature, document properties definitions, or template.	Any
Protocol	Specifies a network protocol or port.	• McAfee DLP Monitor • McAfee DLP Prevent
Discover	Defines the scan using parameters such as scan operation, host IP address, repository type, domain name, and so forth.	McAfee DLP Discover
Endpoint	Defines conditions specific to McAfee DLP Endpoint. This option is not available on the **Exceptions** tab.	McAfee DLP Endpoint
Date/Time	Defines the file by creation time, last modification time, or last access time. This option is not available on the **Exceptions** tab.	Any

Action rule options

Action rules apply preventive or corrective actions when rules generate incidents. The actions available depend on which McAfee DLP product implements them.

When creating a new McAfee DLP action rule, the default action is **None**. This allows you to monitor the system and collect data before deciding which action is appropriate. You can enable notification with any action.

McAfee DLP Prevent must have an action rule configured for the rule to be active.

Table 12-3 Action rule options

McAfee DLP product	Available actions
McAfee DLP Monitor	**Allow**
McAfee DLP Prevent with a proxy server	• **Block** • **Monitor**

Table 12-3 Action rule options *(continued)*

McAfee DLP product	Available actions
McAfee DLP Prevent with a Mail Transfer Agent (MTA)	• **Block** • **Bounce** • **Encrypt** • **Monitor** • **Notify** • **Quarantine** • **Redirect**
McAfee DLP Discover	• **Move** • **Copy** • **Encrypt** • **Delete**
McAfee DLP Endpoint	• **Block** • **Delete** • **Encrypt** • **Monitor** • **Notify** • **Quarantine** • **Request Justification** • **Store Evidence** • **Tag**

Template options

Templates define information that is used repetitively. Standard templates can be used in a wide variety of operations; customized templates are single-purpose.

Table 12-4 Template options

Option	Definition
Name	Required unique template name.
Description	Optional description.

Component Type	Select from the following:
	• Any product:
	  • **Content**
	  • **File Information**
	• McAfee DLP Monitor and McAfee DLP Prevent only:
	  • **Source/Destination**
	  • **Protocol Information**
	  • **Network filter**
	• McAfee DLP Discover only — **Discover**
	• McAfee DLP Endpoint only — **Endpoint**

Construction	Defines the template according to the component type selected.

Concept options

Concepts are used to define sensitive content to match.

There are two categories: **Built-in** and **User Defined**.

Table 12-5 Concept options

Option	Definition
Algorithm	A pre-defined text pattern such as a Social Security number, using McAfee Expressions.
Category	Pre-defined groups, such as **Legal** or **Payment Card Industry**. Select from a list to assign the concept to a category.
Expression	User-defined text or text pattern. In addition to being entered manually, expressions can be imported (uploaded).
Count	Defines a threshold for reporting. The expression must be found at least the specified number of times for an incident to be logged.
Percentage Match	Incidents are not reported unless the expressions are found within the specified percentage of text in a file.
Number of lines from beginning	Incidents are not reported unless the expressions are found within the specified number of lines from the beginning of the file.
Number of bytes from beginning	Incidents are not reported unless the expressions are found within the specified number of bytes from the beginning of the file.
Proximity	Incidents are not reported unless the expressions are found proximate to a specified byte. Options are **Less than**, **Equals**, and **Greater than**.
Advanced	Defines whether content concepts or session concepts are used.

Document property options

Document properties are used to define file information for rule matching. In addition to pre-defined properties, you can define custom properties.

Table 12-6 Document property options

Option	Definition
Name	Name of the property (required). If you define a custom property, you can replace the default name with a more descriptive name.
Description	Optional description. You can add descriptions to both the property and the value.
Value	The text to be matched by the rule. You can specify **Allow Partial Match** for a wider search.

The property **Any Property** allows defining a property by value alone. This feature is useful in cases where the keyword has been entered in the wrong property parameter or when the property name is unknown. For example, adding the value *Secret* to the **Any Property** parameter classifies all documents that have the word *Secret* in at least one property.

Registered document options

Documents with sensitive content are registered by uploading them to McAfee DLP Discover. If files are registered through McAfee DLP Manager, they are automatically registered on all managed devices.

Table 12-7 Registered document options

Registration panel	Description
Web Upload	Displays a list of uploaded files. To upload a file you must specify the file path, registration name, signature type, policy, rule, and device. Size limit is 10 MB per file.
Data Registration	Displays a list of uploaded data files. CSV and compressed CSV are supported. Size limit is 100 MB per file (compressed).
Excluded Text	Displays a list of excluded content. Excluded text is usually boilerplate or other innocuous content. The size limit is 512 characters for each example.

Policy setting options

You can configure policies to throttle incidents or encrypt data.

Table 12-8 Policy setting options

Option	Definition
Configure Throttling Parameters	If a certain number of incidents for a particular rule has been generated within the specified time frame, subsequent incidents are suppressed. By default, incidents for a rule are suppressed if there are more than 30 generated within 60 seconds. Incident throttling is not supported for McAfee DLP Endpoint events.
Security Settings	Specifies data encryption. Available settings are **Encrypt Sensitive Incident Data** and **Encrypt Capture Data**.

13 Integrating McAfee DLP Endpoint

McAfee DLP Endpoint is integrated into the network product suite through the ePolicy Orchestrator or McAfee DLP Manager management console. McAfee DLP Endpoint adds protection for Data-in-Use to the product suite by monitoring and managing devices and user activities at network endpoints.

What is McAfee DLP Endpoint?

McAfee DLP Endpoint is an agent solution that monitors enterprise users' actions through the computers and devices they use in the course of their work. It prevents compromise of sensitive data at a variety of network endpoints — not only on computers, but on removable media, printers, clipboards, screens, windows, and defined shares and paths. Through McAfee DLP Manager, significant events that occur at those endpoints can be delivered to the unified product suite, integrated into the incident workflow, and resolved with appropriate actions.

The software is managed by ePolicy Orchestrator and deployed through a DLP client of McAfee Agent, which distributes policies to endpoints and enforces them by generating and storing significant events in an evidence folder. After the events are accessed by McAfee DLP Manager, they are displayed on the ePolicy Orchestrator and McAfee DLP Manager Data-in-Use dashboards.

Contents

- *How McAfee DLP Endpoint works with McAfee DLP Manager*
- *Setting up McAfee DLP Endpoint*
- *Working with a unified policy*
- *Extending McAfee DLP Discover scans to endpoints*
- *Tagging and tracking*
- *Controlling devices*
- *Working with endpoint events*
- *Typical scenarios*

How McAfee DLP Endpoint works with McAfee DLP Manager

Integration of McAfee DLP Endpoint into the network product suite begins when a trust relationship is established between ePolicy Orchestrator and McAfee DLP Manager. After credentials are used to authenticate the connection, ePolicy Orchestrator extensions for McAfee DLP Endpoint and the network product suite cooperate to allow communication with McAfee Agent (through a client plugin).

When the unified policy is distributed through ePolicy Orchestrator to endpoints and a match is detected, an event is generated at the endpoint. It is encrypted, then delivered through the McAfee DLP client to an evidence folder that is usually located on ePolicy Orchestrator. At pre-defined posting

intervals, McAfee DLP Manager gets events from the evidence folder and displays the objects and attributes (including paths) found on the **Data-in-Use** dashboards. The columns of the display contain specific event attributes and can be rearranged to display only the most significant information.

McAfee DLP Endpoint must be registered to McAfee DLP Manager through ePolicy Orchestrator, and a user account must be created to access the evidence folder.

Any attribute of any event might be used to create a new rule with actions that might find similar events in the future. When the rules are redefined, they are transferred through the unified policy to the global policy, and the updates are then deployed to endpoints through a secure channel maintained by the McAfee DLP client.

Location of McAfee DLP Endpoint features

In McAfee DLP Manager, McAfee DLP Endpoint functionality is located either on the system **Endpoint Configuration** page, or on the rules pages.

Endpoint configuration in McAfee DLP Manager includes tools for setting up the system, controlling devices, and managing application tagging.

Rules pages contain an **Endpoint** category that has parameters that can be added to every rule in the network product suite. After they are configured, the rules are deployed to the network extension, which integrates the global policy into the unified policy design.

Endpoint parameters in unified rules

Because unified policy rules can contain parameters that are deployed separately by all of the McAfee DLP, a single unified rule can be used to monitor traffic, scan repositories, and manage data at endpoints in the same operation. For example, a *Payment Card Industry* policy that has been deployed through McAfee DLP Manager can be used to identify privacy violations in network traffic, in data repositories, and on endpoints.

Multiple endpoints can be added to a rule as a group by creating a template, then selecting it from the menu before saving the rule. Adding frequently used collections of endpoints to a rule increases its efficiency and scope.

Setting up McAfee DLP Endpoint

Before McAfee DLP Endpoint can be integrated with the global McAfee DLP policy, you must install the software and perform initial configurations.

Installing McAfee DLP Endpoint

McAfee DLP Endpoint must be installed before it can be integrated with other McAfee DLP products.

For information and instructions on installation, see the *McAfee Data Loss Prevention Endpoint Software Installation Guide*.

Configure McAfee Agent on ePolicy Orchestrator

You must add an evidence folder on ePolicy Orchestrator to collect the events forwarded by the McAfee Agent client, then configure essential features to enable McAfee DLP Endpoint functionality through McAfee DLP Manager.

Task

1 In ePolicy Orchestrator, select **Menu** | **Policy** | **Policy Catalog**.

2 From the **Product** menu, select **Data Loss Prevention 9.2: Policies**.

3 Locate the **McAfee Default Agent Configuration** and click **Duplicate**.

4 Enter a name for the policy, then click **OK**.

5 From the list of policies, select the duplicate policy.

6 In the **Evidence** tab, type the UNC Path of the evidence folder share and folder name.

```
\\server name\evidence
```

The same server will also be entered on the McAfee DLP Manager **Add New Evidence Server** page.

7 Select **Copy evidence using NETWORK SERVICE or logged on user**.

8 In the **Evidence Replication** section, select the **Evidence** and **Hit Highlighting** checkboxes.

Show abbreviated hits appears in the associated field.

Enabling this option allows users to easily see matching text in the events reported to the McAfee DLP Manager **Data-in-Use** dashboards.

9 In the **Security** tab, enter a list of authorized users and groups to enable manual tagging of files on agent machines.

For example, enter **Everyone** to give **Manual Tagging Authorization** to all users.

This sets up the agent to support manual tagging through McAfee DLP Manager. Selecting the **Allow Manual Tagging** checkbox when creating tags on the **Endpoint Configuration** page makes the tags visible to trusted users, who can use them to classify documents on their desktops.

10 Click **Save**.

Add an evidence folder on ePolicy Orchestrator

To collect the events forwarded by the McAfee Agent client, add an evidence folder on ePolicy Orchestrator.

If an evidence folder is not already installed on ePolicy Orchestrator, you must add one to communicate with the evidence folder on McAfee DLP Manager.

Task

1 In ePolicy Orchestrator, click **Policy Manager**.

2 On the **Agent Configuration** page for the McAfee DLP product, click **Edit Settings**.

3 Under the **Evidence** setting, type the evidence folder share and folder name.

```
\\server name\evidence
```

This information will be entered on the McAfee DLP Manager **Add New Evidence Server** page.

4 Review the other agent settings and make changes as appropriate.

5 Click **Save**.

Configuring McAfee DLP Endpoint on McAfee DLP Manager

After McAfee DLP Endpoint and its components are installed on ePolicy Orchestrator, you must configure the system to start detecting endpoint events through McAfee DLP Manager.

After McAfee DLP Endpoint is integrated McAfee DLP Manager, the following tasks must be completed before McAfee DLP Endpoint can work with the network product suite.

- Enable unified policy management by generating a policy, setting a posting period, and selecting a backward compatibility mode.
- Add an agent override password to encrypt and decrypt evidence and override default reactions.
- Add a list of printer models that cannot be controlled by McAfee DLP software.
- Create tags, then set up optional manual tagging.

When these operations are complete, you can define unified rules on the **Policies** page, then view the **Incidents** | **Data-in-Use** dashboard to verify that the endpoint events are being generated and reported.

Click the **Columns** icon, then add or remove columns to display exactly the information that is needed.

Maintaining compatibility with installed agents

McAfee DLP Manager is capable of supporting multiple versions of McAfee DLP Endpoint at the same time.

McAfee DLP Endpoint was previously known as McAfee Host DLP.

The compatibility mode is selected on the **Manage Endpoints** page.

- **DLP Agent 9.0 and above** is the default endpoint management configuration option and should be selected if McAfee DLP Manager must support earlier versions.
- **No compatibility** should be selected if earlier versions do not need to be supported. This option allows full functionality of the current version.

The need for digital rights management, which controls use of digital content not authorized by the content provider, might be an additional consideration. This feature of McAfee DLP Endpoint is not supported in McAfee DLP Manager, so network and endpoint applications might have to be run separately.

Generate a global policy for McAfee DLP Endpoint

When you manage endpoints from McAfee DLP Manager, you must generate a policy, set a posting interval, and select a compatibility mode. These settings support the distribution of McAfee DLP Endpoint events to McAfee DLP Manager dashboards through ePolicy Orchestrator.

Rule definitions for McAfee DLP Endpoint were originally designed to share a single global policy definition — only one policy supported multiple rules. But McAfee DLP Manager is designed around a collection of unified international policies, and the McAfee DLP Endpoint global policy is accommodated within that system.

If McAfee Host DLP is already installed on ePolicy Orchestrator, using the McAfee DLP Endpoint networked version will overwrite the events on the evidence server. Because of this potential problem, you must deliberately generate a policy to support installation of the updated endpoint product.

You must also set an interval for posting policy modifications through ePolicy Orchestrator. By default, rule definitions are updated on the McAfee DLP Endpoint extension every 30 seconds, but you can define a more conservative transfer interval (up to two hours, or 7200 seconds) by editing the **Time Duration for Posting Policy Definition** setting.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration** | **Miscellaneous** and click **Manage Endpoints**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration** | **Miscellaneous** and click **Manage Endpoints**.

2 Select the **Generate Policy for Endpoint** checkbox.

3 In the **Time Duration for Posting Policy Definition** field, enter a number between 30 and 7200 seconds.

The policy is generated, posted from McAfee DLP Manager to ePolicy Orchestrator, saved in the database, forwarded to the connected agents, and updated at the defined interval.

4 Click **Submit**.

Add an Agent Override password

You must set an **Agent Override** password before working with McAfee DLP Endpoint. It is used with McAfee DLP Agent to generate authentication codes that are needed to approve agent override requests.

McAfee DLP Endpoint generates agent override requests when operations that require authentication are attempted. For example, you might want to release quarantined files, or encrypt and decrypt evidence.

Such operations require users to provide two types of authentication — an ID Code and a Release Code.

- The ID Code is generated by McAfee DLP Agent, which uses the Agent Override Password with an algorithm to calculate a code. That number automatically populates a field in a pop-up that is launched whenever authentication is required.
- The Release Code must be provided by an ePolicy Orchestrator administrator, and this code must be provided verbally during an offline call.

When both codes are entered into the fields in the pop-up, the Agent goes into bypass mode, and the operation is allowed.

If McAfee Endpoint Encryption for PC is installed, a pop-up might prompt the user for a key that is generated by that product.

However, if a **Request Justification** pop-up is launched when a file is opened, a password is not required. The user simply types in an justification, and the administrator monitors the text entries periodically.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration** | **Miscellaneous** and click **Agent Override Password**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration** | **Miscellaneous** and click **Agent Override Password**.

2 Enter a password in the **Password** field and confirm it.

This sets up a password that is used by McAfee DLP Agent to generate an ID Code.

3 Click **Submit**.

Define unmanaged printers

Because some printers might not work with the proxy driver architecture required for McAfee DLP management, they should be whitelisted and excluded from management by the system.

Unmanaged printer definitions are created by selecting printer model information from the Active Directory server pop-up menu. There might not be any printers in your organization that cannot be managed, so this is an optional operation.

If you have not added an Active Directory server to the system, type printer paths and names to be whitelisted in the **Printer Model** field, then click **Add Printer**.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sysconfig** | **Endpoint Configuration** | **Miscellaneous** and click **Unmanaged Printer Models**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration** | **Miscellaneous** and click **Unmanaged Printer Models**.

2 Click **?**, then **Find**, and select from an existing **Directory Server** list.

3 Click **Apply**.

4 Click **Add Printer**.

Set the manual tagging option

If you have administrative privileges, you can apply tag labels to allow trusted users to classify specific documents. If the **Allow Manual Tagging** checkbox is selected during that process, the tag is visible to your trusted users, who can use it to classify specific documents by applying the appropriate tag.

Before you begin
McAfee DLP Endpoint and its components must be set up on McAfee DLP Manager.

After they are created, manual tags are pushed to users at endpoints by the McAfee Agent client.

The ability to classify documents with tags encourages users to take independent action to protect files within their areas of responsibility. For example, users at medical facilities might be trusted to apply HIPAA tags to patient records that must be kept confidential by law.

If the **Allow Manual Tagging** checkbox is not selected, file tagging can still be done manually — but only by administrative users, who can tag or remove files individually or in groups.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Endpoint Configuration** | **Application Definition** | **Tag Labels**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Endpoint Configuration** | **Application Definition** | **Tag Labels**.

2 Select a tag.

3 Select the **Allow Manual Tagging** checkbox.

4 Click **Save**.

Working with a unified policy

In McAfee Host DLP, rule definitions share a single global policy definition for all rules. In the unified policy design, the global policy is used to add McAfee DLP Endpoint functionality to the network product suite.

The networked products protect email and webmail through the unified rules, but there is some duplication of functionality because McAfee Host DLP (McAfee DLP Endpoint) already protected that data.

Unified rules specifically incorporate **Endpoint** parameters, such as the protection rules and tagging, but the **Content** category and much of the **Source/Destination** category contain additional parameters that can be used on endpoints as well as networks. For example, the GeoIP location feature is supported only by the network products.

The unified rules can also use data captured by McAfee DLP Monitor or scanned by McAfee DLP Discover scans to adapt to changing conditions.

Because all of these capabilities are integrated into the unified policy design, one rule can be configured to add incidents and events to all three dashboards (**Data-in-Motion**, **Data-at-Rest**, **Data-in-Use**). For example, a *Payment Card Industry* policy that has been deployed on McAfee DLP Manager can be used to identify privacy violations in network traffic, in data repositories, and on endpoints.

You can use templates to add frequently-used actions and conditions to a rule, increasing its efficiency and scope. If the rule is to be applied to endpoints, select **Template** from the **Endpoint** category and click **?** to launch the available selection. If none are available, add a new one on the **Policies** | **Templates** | **Add Template** page using the **Endpoint** component type.

Endpoints might be computer- or user-defined, but computer assignment groups are outside of the scope of unified policy management, and can only be defined in ePolicy Orchestrator. Endpoints can be monitored from McAfee DLP Manager by adding user-based parameters (such as groups and organizational units) to a rule.

Unified policy content strategy

Because the network product suite uses a classification engine that differs from that used by McAfee DLP Endpoint, a different content strategy is used to deploy unified rules to endpoints.

McAfee DLP Endpoint uses built-in dictionaries with terms that are commonly used in health, banking, finance, and other industries, and text patterns that identify known strings and complex patterns through the use of POSIX regular expressions. File properties and registered document repositories, which are identified by location-based tags, are also used to classify content, and whitelists define text that should be ignored by the tracking mechanism.

The McAfee DLP Monitor classification engine sorts all data into content types and stores it on the McAfee DLP appliances. Data is also classified by source and destination (including geographic location), file properties, protocols, and database components (including data sorted into tables, columns and rows), and because it is analyzed and parsed, it can also be queried.

The attributes of the captured objects can be viewed on any rules page on the unified policies dashboard, and the same rule definitions can be used to find incidents and violations in network traffic, data repositories, and on endpoints. Actions can also be pre-programmed to resolve incidents and events for all three types of data.

Because of these differing data designs, endpoint parameters can be combined with all of the network product parameters that can be defined in unified rules. There is no need for repetitive rule setting, since all protection rules can use the same defined parameters.

In a unified policy, rules that have a **Content Type** specified might match similar file types, even if that file type is not specified. For example, if a rule has a **Content Type** of JPEG specified, matching connections with other image types, such as BMP or GIF, will trigger the rule.

Integration into the unified workflow

McAfee DLP Endpoint events are integrated into the same workflow as McAfee DLP Monitor, McAfee DLP Discover, and McAfee DLP Prevent.

Through McAfee DLP Manager, all of the McAfee DLP products share the ability to view, group and filter results in different configurations, get details on the attributes of the objects found, prepare reports, and manage related events by adding them to cases.

Events detected at network endpoints are stored in an evidence folder and copied over to McAfee DLP Manager in a data stream. Because they are not indexed, they are not searchable, but the data shares all other aspects of the unified workflow.

How McAfee DLP Endpoint rules are mapped

When McAfee DLP Endpoint was integrated into McAfee Data Loss Prevention, its global policy and existing rule structure had to be adapted to the unified policy design.

In the networked product suite, rules are organized under many sets of international policies that can have multiple owners. Unified policy design preserves this hierarchy by feeding McAfee DLP Endpoint parameters into this structure as attributes, or rule types. The merged structure is changed to `<policy owner> <policy> <rule> <rule type>`.

Adding endpoint parameters to rules in McAfee DLP Manager

When added to the existing rules in the product suite, endpoint parameters can be used to extend internationalized standard or customized rules to computers, removable media, printers, clipboards, screens, windows, shares and paths.

Protection rules

Protection rules can be added from the **Endpoint** category on the **Add** or **Edit Rule** page. They include reactions that vary depending on a number of conditions, including whether the user is on- or off-site. For example, a user who attempts to upload a file to a social media site might be prevented from doing so by implementing the *Web Post Protection Rule*, which can be configured to send notification of the event and store evidence relating to it.

Protection rules define the reactions that are to be taken when an attempt is made to transfer or transmit tagged data. Each protection rule can deploy different combinations of actions, which can be viewed by selecting an action rule under **Policies** | **Action Rules** | **Data-in-Use**.

Exceptions

If a unified rule contains attributes that are not supported by McAfee DLP Endpoint, the rule will not produce accurate results. Do not use the following attributes in rules that are deployed to endpoints.

- Email address sender variants
- Email subject (except for the condition **contains none of**, which is supported)
- GeoIP locations
- User city
- User country
- File size

- Keyword *expressions*
- Concept *expressions*

Keywords and concepts used with **any of**, **all of**, and **none of** conditions are used are supported (as are keywords defined by exact phrases). Only the keyword and concept expression *condition*, which is used to build complex command line queries using logical operators, is unsupported.

Add endpoint protection to existing rules

You can add protection to existing unified rules by adding **Endpoint** parameters.

Open the **Endpoint** component on any **Edit Rule** page to see what parameters are available.

For example, you might add a **Protect Network Printers** parameter to an existing *Banking and Financial Sector* rule to block endpoint computer users from printing sensitive financial data.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** and click any rule under any policy.
   - On your McAfee DLP appliance, select **Policies** and click on any rule under any policy.

2 Open the **Endpoint** component.

3 Select an endpoint parameter and define it. If it is a protection rule, click **?**, then select **Enable** and **Apply**.

   Protection rules are disabled by default.

4 If a reaction is to be added, click the **Actions** tab, then **Add Action**.

5 Select a suitable action from the **Data in Use** section.

6 Click **Save**.

Assign events to cases

If further investigation is warranted, you can assign events to the same cases as **Data-at-Rest** and **Data-in-Motion** incidents.

If an error is encountered while assigning incidents to a case (for example, the object cannot be fetched from the evidence share), you must reassign each of the failed incidents to the case.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.

2 From the **Data-in-Use** dashboard, select one or more endpoint events.

3 Click **Assign to Case** and select **New Case** or **Existing Case** from the sub-menu.

4 Click **Apply**.

Using protection rules in McAfee DLP Manager

You can deploy discovery, application, and web post protection rules to endpoints by adding them to unified rules. You can deploy the reactions associated with them by adding action rules.

The reactions applied by protection rules have become **Data-in-Use** action rules in McAfee DLP Manager, and they are disabled by default. Before a protection rule can be added to a unified rule, it must be selected from the **Endpoint** category on the **Edit Rule** page and **Enabled** on the pop-up menu.

Protection rule reactions are defined on the **Action Rules** page under **Data-in-Use**. The following actions are available:

- Block
- Delete
- Encrypt
- Monitor
- Notify User
- Quarantine
- Request Justification
- Store Evidence
- Tag

There are limitations on reactions that can be used in the same action rule. For example, Block and Encrypt actions cannot be used in the same rule. You can find a complete list by clicking **Tips** on the **Policies** | **Action Rules** | **Add Action Rule** page, which launches the **Endpoint Action Rule Constraints** pop-up.

When combined with **Data-in-Motion** and **Data-at-Rest** action rules, one unified rule can act on data anywhere — on- or off-site (*online* and *offline*).

Add a reaction

Add a reaction by adding a **Data-in-Use** action rule.

If multiple actions are selected, they will be applied simultaneously when an event is detected. For example, a **Removable Media** reaction might block, monitor, and store evidence of a significant event, whether the device is on- or off-site.

Task

1. Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
   - On your McAfee DLP appliance, select **Policies** | **Action Rules**.
2. From the **Actions** menu under **Data-in-Use**, select **Add Action Rule**.

   Endpoint actions can be taken if the detected device is on- or off-site (*online* or *offline*). Select one or both.
3. Enter a name for the action rule.
4. Select one or more actions to be taken.

   If the event detected is to be encrypted, provide an encryption key. Consult the updated *Endpoint Encryption for Files and Folders 4.0 Product Guide* for more information.

   If the event detected is significant, select a **Severity** from the drop-down list.

   If users are to be notified when the event is detected, enter a message. Entering link text or a URL is optional.
5. Click **Save**.

   After you have created the endpoint action rule, apply it to one or more rules.

Apply a reaction

Apply a reaction by selecting a **Data-in-Use** action rule and adding it to a rule.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** and click on a rule that has one or more endpoint parameters.
- On your McAfee DLP appliance, select **Policies** and click on a rule that has one or more endpoint parameters.

2 Click the **Actions** tab and select **Add Action**.

3 Select one or more **Data-in-Use** actions to be taken when a protected endpoint is detected.

4 Click **Save**.

Extending McAfee DLP Discover scans to endpoints

Registered index packages found by McAfee DLP Discover are shared with other McAfee DLP appliances, and also with the McAfee DLP client, which distributes them to endpoints and controls files containing registered content.

McAfee DLP Endpoint uses document registration and location-based tagging to identify sensitive data at rest on endpoints. Confidential files that were created after a tag was applied to a group of files might not be detected by a rule, so they could be accessed by an endpoint user. But if the location is scanned, those files at risk will be protected because they are in a defined location path.

Applying tags by scanning

Many files can be tagged in a single operation by using a Discover CIFS scan to crawl Windows shares that serve computers and mounted volumes. The unified policies defined in the Discover operations apply rules against the data at rest on endpoints, and when a match is found, a tag is added as metadata to any file that meets the conditions of the rule.

When a McAfee DLP Manager Discover scan is run on a CIFS share, endpoints are automatically included in the network scan by virtue of the unified policy design.

Tagging files in data at rest or in use is a two-phase process when McAfee DLP Discover is used to apply tags. Although the definition of the scan and the policies to be used to detect sensitive data are set on the network side, the scheduling of the scan, the credentials used, and other scan definitions must be set through ePolicy Orchestrator on the **Agent Configuration** page.

How signatures used at endpoints are stored

McAfee DLP Manager generates signatures when significant data is found through matching text patterns, regular expressions, content types, keyword expressions, and built-in or user-defined concepts to dynamic and static data. The results of those matches are stored in *DBReg* and *DocReg* concepts that function as *signature banks*.

The contents of these two concepts, which store signatures for structured and unstructured data, are automatically shared across all McAfee DLP appliances. If you add the two signature banks to unified rules, you can use the registered data they contain to match the same sensitive data on network endpoints.

Scanning local drives

When a Discover scan operation is defined on McAfee DLP Discover through McAfee DLP Manager, the scan is extended to local drives. The connection to users' computers is made through unified policies, which are defined in the Discover scan and deployed to both network locations and endpoint file systems.

It is not possible to tag all files at risk on computers, and any mounted volumes, but Discover scans of CIFS (Windows-based) shares can be used to deploy rules to any file found on C$ (the local drives) through that share. Using this method, McAfee DLP Manager can identify and tag potential problems on large volumes of endpoint files.

But scans of endpoint computers can only be constructed in McAfee DLP Discover, and scans cannot actually run until the conditions defined on the **Agent Configuration** page in ePolicy Orchestrator are met. After the scan completes, the results are returned to McAfee DLP Manager through the secure channel maintained by the McAfee DLP client.

Scan data at rest on endpoints

Discovery scans on computers and mounted devices (such as USB and extended drives) are configured using McAfee DLP Discover to create a CIFS Discover scan. But the scan is actually run through ePolicy Orchestrator by configuring the scan definition (schedule, credentials, etc.) on the **Agent Configuration** | **Discovery Settings** page.

Before you begin

Determine which policies you are going to use to scan endpoints, and deploy them by selecting the **Host** checkbox on the policy page. All rules of the policy must be enabled so that they can inherit the state of the policy.

Because ePolicy Orchestrator is a Microsoft Windows server, the Discover scan must be configured to use the CIFS protocol.

The network-based Discover scan is used as a framework for endpoint scans. Since scan definitions are defined by configuring the agent, those parameters should be skipped in the **Edit Scan Operation** pages.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 In the **Actions** tab, select **New**.

3 Type in a scan task name and optional description.

4 From the **Repository Type** menu, select CIFS.

Do not make a selection from the **Credential** and **Schedule** menus.

5 From the **Mode** menu, select the Discover scan type.

6 Under **Devices**, select the McAfee DLP Discover appliance from which the scan will be run.

7 In the **Node Definition** tab, provide the IP address of the CIFS server that is the target of your scan.

8 If you want to test the connection, select your device before clicking **Test**.

9 Click **Include** to add the defined node to the **Included** list.

If you want to exclude one or more addresses from an IP adress range or subnet, click **Exclude**.

10 Click the **Filters** tab to define the exact location on the server that you want to scan.

You can filter by share, folder, and file property on CIFS server.

11 Click **Browse** to navigate to the location of the scan.

Alternatively, open the **Filter** category and set the options manually.

12 Click the **Policies** tab and select policies whose rules will be applied against data at rest in the defined repositories.

13 Click **Save**.

Tagging and tracking

A tag is metadata that is added to a file in the form of a Globally Unique Identifier (GUID), and it can also have a name and description. Tags are essentially extended attributes that can be used to identify and track sensitive content on computers, removable media, and other devices that contain data.

Tags work as classification devices and stay with the content, even if it is copied into another document, moved to another location, attached to other files, or saved to another format.

A tag label can be either application- or location-based, and in McAfee DLP Manager, might be applied in one of three ways:

- By rule (automatically)
- Directly (manually)
- By scanning a Windows repository (automatically)

After tags are created, the files to which they are applied can not only be tracked, but controlled by pre-programming **Data-in-Use** action rules that fire when tagged objects are found.

Using tags

In the network product suite, unified rules might contain location or application-based tags. They might be used alone, or in combination with other parameters to identify and apply actions to data at risk anywhere within the reach of the McAfee DLP Manager.

Users who have administrative privileges can create **Tag Labels** on the **Endpoint Configuration** page, then select them from menus on **Edit Rules** pages to define a condition for automatically applying them. If used on those pages, they can also be added automatically to CIFS (Windows) repositories and endpoints through Discover scans.

When tag labels are used on unified rules pages, they can be applied as needed to files that match the conditions of the rules, or existing tags can be applied to a specific set of files that are defined by the rule.

For example, the Pharmaceutical Industry *Drug Code Data* rule might be modified to include an **Existing Tag Label** that identifies and tracks any document containing that code. An *Email Protection Rule* might then be added to prevent users from sending those documents to competitors.

This particular rule applies only to data in motion, but email protection is covered by all McAfee DLP products.

Applying tags with unified rules

Many files can be tagged in a single operation by using tags in combination with unified policy rules.

When a tag is added to a network rule, it is not only extended to endpoints, but it can be used to impose a wide variety of conditions on the targeted data before the tag is applied.

Many different network and endpoint parameters might be used to automatically apply tags when sensitive data is detected — and if specific conditions are not met, they might not be applied at all.

For example, a network rule might be used in an Asian bank to find and apply privacy tags to all files that contain *China UnionPay* credit card numbers. But the administrator might want to tag those files only if they are being posted to a known "carders" web site by an insider who is under investigation.

In such a case, the rule might contain a user name selected from an LDAP server, and the *HTTP_Post* protocol might be added to establish criminal intent. If both of those conditions are found, an **Existing Tag Label** would be automatically applied, and a **Web Post Reaction** action rule might also be applied to block the attempt and store evidence.

Applying tags manually

Tag labels can be added by any user who has administrative privileges. If the **Allow Manual Tagging** checkbox is selected during that process, the tag is visible to trusted users, who can use it to classify specific documents by applying the appropriate tag. After they are created, manual tags are pushed to users at endpoints by the McAfee Agent client.

The ability to classify documents with tags encourages users to take independent action to protect files within their areas of responsibility. For example, users at medical facilities might be trusted to apply HIPAA tags to patient records that must be kept confidential by law.

If the **Allow Manual Tagging** checkbox is not selected, file tagging can still be done manually — but only by administrative users, who can tag or remove files individually or in groups.

Application-based tagging

Tags that identify applications are applied when a file is saved using a specific application, and the tag displays whenever the user opens the file. When used with other properties of a unified rule, they can be used to control files created by that application.

Simple application-based tagging rules monitor or block all files created by the application, but addition of other rule parameters can qualify or extend those actions when used in a more specific context.

Application tagging might be only one property of a unified rule. When an application definition is applied, or applications sharing a particular strategy are used (for example, all applications are editors), an application tag might be applied to a group of documents.

How application tagging works

Applications can be deployed with tagging and protection rules by creating application definitions, then applying them to unified rules. They can also be applied manually, or by using a Discover CIFS scan.

Importing an applications list and creating application definitions are efficient ways of handling application-related tagging and protection rules.

For example, system administrators might import a list of all relevant applications available within the enterprise, create application definitions based on their needs, and implement these definitions with relevant rules to maintain policies.

When a user opens files with an application that is defined in a rule by an application definition, it produces one event on the McAfee DLP Monitor *per application session*, not per sensitive file opened. The event includes all files that matched the specified conditions in that application session. For example, if the **Store Evidence** parameter is selected on the **Data-in-Use** action rule page, only files from the current session are stored.

The Enterprise Application List

The Enterprise Application List contains a set of commonly-used applications. You can add applications to the list, delete them, or add an application definition that bundles related applications.

When an application is added to the Enterprise Application List, application-based tags are applied to matching files when they are found.

Applications must be defined in the Enterprise Applications List before they can be referenced in a rule. If the applications you want to use do not appear on the list, you must add them.

When an Endpoint application tag is used with unified rule parameters and associated action rules, files that are detected on endpoints, in network traffic, and repositories can be controlled with one rule. Application-based tags might be used alone or collected in application definitions.

For example, users who open Adobe Photoshop files on endpoints or on network shares might be allowed to view, but not modify those files — or they might not be visible at all. But before building such a rule, the .psd executable file would have to be added to the Enterprise Action List so that it is available for use in a unified rule. Once Photoshop files are defined as significant objects and supplemented with other parameters, they can be detected and tagged when the unified rule is run, and an appropriate action might be taken at that time.

Strategies for categorizing applications

McAfee DLP Endpoint software divides applications into four categories or *strategies*.

A strategy is assigned to each application definition. You can change the strategy to achieve a balance between security and the computer's operating efficiency. The strategies, in order of decreasing security, are:

- **Editor** — Any application that can modify file content. This includes "classic" editors like Microsoft Word and Microsoft Excel, as well as browsers, graphics software, accounting software, and so forth. Most applications are editors.
- **Explorer** — An application that copies or moves files without changing them, such as Microsoft Windows Explorer or certain shell applications.
- **Trusted** — An application that needs unrestricted access to files for scanning purposes. Examples are McAfee® VirusScan® Enterprise, backup software, and desktop search software (Google, Copernic, and so forth).
- **Archiver** — An application that reprocesses files. Examples are compression software such as WinZip, and encryption applications such as McAfee® Endpoint Encryption for Files and Folders software or PGP.

Change the strategy as necessary to optimize performance. For example, the high level of observation that an editor application receives is not consistent with the constant indexing of a desktop search application. The performance penalty is high, and the risk of a data leak from such an application is low. Therefore, you should use the trusted strategy with these applications.

Add a file extension parameter

File extensions can be defined along with other endpoint parameters to control applications by type.

Before you begin

Check to see if the file extension parameter already exists on the **Endpoint** file extension pop-up menu. If not, you can add it by entering it in the **Original Executable File Name** pop-up menu on the **Create Application Definition** page, which will add it to the **Enterprise Application List**. The added file type can then be selected from the **Application Definition** pop-up menu.

Suppose you want to implement role-based access on a Windows network engineering share. You might have developers who have full access, users who are allowed to manage the contents of the site, and users who have special skills that are needed on specific document types.

For example, a group of technical illustrators might need access to the Adobe Photoshop and Illustrator files on that share. You could create a rule that would allow only those users access to those files.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **User Groups** from the **Source/Destination** menu, and click **?**.

4 From the directory server pop-up menu, click **Find** and click the technical illustrators' user group.

5 Click **Apply**.

6 From the **Endpoint** menu, select **File Extension**, click **?**, and select the applications from the pop-up menu.

In this use case, the PSD file type is listed, but you would have to add the AI file type in advance.

7 Click **Apply**.

8 From the **Endpoint** menu, select **Network Path**, click **?**, and use **Find** to select the share that contains the files.

9 Click **Apply**, then **Save**.

Protect data using an application-based tag

You can use an application protection rule to keep users from modifying or distributing all Microsoft Office documents on a protected Windows share.

Before you begin

If you want to use an **Existing Tag Label**, you must first create one on the **Endpoint Configuration** page.

Suppose you have a collection of *Health Insurance Portability and Accountability Act Compliance* documents that must be not only be kept confidential, but must not be modified in any way.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy and rule are in an **Enabled** state.

3 On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

The concepts palette appears.

4 From the **Source/Destination** menu, select **User Group** and click **?**.

5 Click **Find**, then click the user group that is to be restricted.

The user group is added to the value field.

6 From the **Endpoint** menu, select **Network Path** and click **?**.

7 Click **Find**, then click the share containing the HIPAA documents.

8 Click **Apply**.

The share is added to the value field.

9 Add an **Endpoint** parameter by clicking **+**.

10 Select **Tags — Application Based** and click **?**.

The **Application Definition** pop-up menu appears.

The **Application Definition** condition can be used for the *Application Protection Rule* or combined with application tagging.

11 Click **Apply**.

12 Click **+** to add another element.

13 Select **Apply Tag Label** and select a tag from the pop-up menu.

14 Click **Apply**, then **Save**.

Application definitions

Application definitions consist of groups of related applications. They are bundled by type to facilitate their use in unified rules.

When an application definition is created, it is automatically added to a template that can be used in rules to find any files created by the applications in the defined group.

Application definitions can be identified by any of the following parameters:

- **Command line** — Allows command line arguments, for example: `java-jar`, that can control previously uncontrollable applications.
- **Executable file hash** — The application display name, with an identifying SHA-2 hash.
- **Executable file name** — Normally the same as the display name (minus the SHA-2 hash), but could be different if the file is renamed.

- **Original executable name** — Identical to the executable file name, unless the file has been renamed.
- **Product name** — The generic name of the product, for example Microsoft Office 2003, if listed in the executable file's properties.
- **Vendor name** — The company name, if listed in the executable file's properties.
- **Window title** — A dynamic value that changes at runtime to include the active filename.
- **Working directory** — The directory where the executable is located. One use of this parameter is to control U3 applications.

With the exception of the SHA-2 applications, all parameters accept substring matches.

You can add applications to application definitions from the Enterprise Applications List, or create them directly.

The same application can be included in several application definitions, and can therefore be assigned more than one of the four strategies. McAfee DLP Endpoint software resolves potential conflicts according to the following hierarchy of application types: archiver > trusted > explorer > editor. In other words, editors have the lowest ranking. For example, if an application is an editor in one definition and anything else in another, McAfee DLP Endpoint software does not treat the application as an editor.

Default application definitions

A set of default application definitions, which consist of related applications that share certain characteristics, is included with the products. They are used to detect the application types in use at endpoints.

Email client applications

The email client applications definition includes the following standard email applications:

- Becky! Internet Mail
- Eudora
- Foxmail
- Microsoft Office Outlook
- Mail Warrior
- Mulberry
- Sylpheed
- The Bat!
- Thunderbird

Encryption applications

The encryption applications definition includes the following standard encryption applications:

- Advanced File Security
- BCArchive
- BCArchive UnPack Application
- Cryptainer
- Cryptainer LE
- Dekart Private Disk Light
- EasyEncipher
- File Manager
- MegaCipher
- Personal Data Vault

- CryptoForge
- CryptoMailer
- Secure IT
- Universal Shield

IM applications

The instant messaging applications definition includes the following standard IM applications:

- AIM
- ICQ
- Skype
- Windows Live Messenger
- MSN Messenger
- Microsoft Office Communicator
- Yahoo! Messenger

Media burner applications

The media burner applications definition includes the following standard burning applications:

- Nero Burning
- Roxio Creator
- Express Burn
- Power2Go
- DVD Movie Factory
- NTI Media Maker
- Gear CD-RW
- Acoustica MP3 CD Burner
- Slysoft CloneCD
- Alcohol 120%

Microsoft Office applications

The Microsoft Office applications definition includes the following standard Microsoft Office applications:

- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office Outlook

P2P applications

The peer-to-peer applications definition includes the following standard P2P applications:

- BitTorrent
- eDonkey
- eMule
- iMesh
- Kazaa
- MakeTorrent
- QT2
- Shareaza
- WinMX

Scanners and indexers

The scanners and indexers applications definition includes the following standard search applications:

- Copernic Desktop Search
- Google Desktop
- Microsoft Windows
- SFXCAB
- X1 Technologies

Web browsers

The web browser applications definition includes the following standard browser applications:

- Amaya
- Firefox
- Google Chrome
- Opera
- Safari
- Windows Internet Explorer

Zip applications

The zip applications definition includes the following standard compression applications:

- WinRAR
- WinZip
- Zipper

Add an application definition

Application definitions control related applications and can be used in rules to control files created by those applications. For example, you might add a definition that includes all applications published by a single vendor, such as Adobe Systems.

You can add application definitions by first adding their executables to the **Enterprise Application List**, then collecting them in an application definition for use in unified rules.

The **Edit Definition Parameter** value fields can contain only one value per field. AND and OR conditions are not supported.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Application Definition**, select **Application Definition List**.

The available application definitions appear in the right pane.

3 From the **Actions** menu, select **Add New**.

The **Add Application Definition** window appears.

4 Type in a name and optional description for the new application definition.

5 Select a **Parameter Name** checkbox from the available list.

This defines the characteristics of the applications being defined. For example, you might select **Vendor Name** for all applications published by Adobe Systems.

The **Edit Definition Parameter** dialog box appears.

6 Click **Save**.

7 On the **Application Definitions** page, select the checkbox of the new definition.

8 From the **Actions** menu, select a **Process Strategy**.

This assigns the definition to a group of application types.

Add a web definition application

Web application definitions allow you to create URL-based templates that enable tagging of files, screenshots, or clipboards saved from one or more web sites.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Application Definition**, select **Application Definition List**.

The available application definitions appear in the right pane.

3 From the **Actions** menu, select **Add New**.

The **Add Web Application Definition** window appears.

4 Type in a name and optional description for the new web application definition.

5 Select a **Parameter Name** checkbox from the available list.

The **Edit Definition Parameter** dialog box appears.

6 Select or enter values that define the parameter.

Click **+** to add additional parameters.

7 Click **Apply**, then **Save**.

Location-based tagging

Location-based tags identify protected shares that contain confidential files. If downloaded to desktops, those files are automatically tagged.

For example, users who do not belong to an executive group might attempt to copy and distribute documents from a restricted executive share. In that case, location-based tags are automatically applied to record the attempt to access confidential information. Pre-programmed actions, such as block, notify, and store evidence, might also be activated when the location tag is applied.

Location-based tags are most often implemented to prevent unauthorized users from accessing shares that contain sensitive data.

Protect data using a network path

The **Network Path** parameter can be used to ensure that a network share containing confidential files is protected. It is used to prevent modification of documents while they are on that protected share. By contrast, the **Location Path** parameter is used to tag files that are copied from a local share to a desktop.

Before you begin

If you want to tag sensitive files, create a tag label under **Endpoint Configuration**, or use an existing one. If you want to trigger an action when the rule hits, make sure that the action rule you intend to use has the right action settings. If not, add a **Data-in-Use** action rule, or create a new one.

If you have to keep a specific file system secure (for example, a share containing forensic records that must be preserved intact), you can type a network path, or select one from a directory server, and use an action rule to prevent them from being modified.

If you just want to identify files that are downloaded from a location path, you can tag them during the download process, then use that tag to control what can be done to them. For example, you might want to allow download but not allow users to modify them. In that case, you can use rules and action rules to locate the tagged files and apply the desired reaction.

If you want to keep sensitive documents on specific shares from being downloaded or compromised, you might give them a collective tag (for example, *Human Resources*) that can be used in combination with an action rule to prevent download or modification. You could tag each document on a share manually, but you could also use that tag with a discovery scan to control similarly-tagged documents in unknown locations.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Add a new policy and rule, or open existing ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

The **Edit Rule** page appears.

3 Open the **Endpoint** category and select **Network Path** or **Tag - Location Path**, then click **?**.

The LDAP server menu appears.

4 Select the directory server, click **Find** on the **AD pop-up**, and select a network location.

5 Click **Apply**.

6 Click the **Action** tab, **Add Action**, and select an action from the **Data-in-Use** list.

In this case, you might want to block the documents, whether they are found *online* or *offline* (in computers that are on-site, or disconnected from the network), and notify a manager.

7 Click **Apply**, then **Save**.

Protect data using a location-based tag

You can use location-based tags to ensure the protection of privileged information on a local share.

If you use a location tag to protect a location, you must define two **Endpoint** parameters: the tag and the location path.

For example, a manufacturing organization might have process engineers working on design documents on computers that are accessed through a share on a Microsoft Windows server. If users who attempt to access and email those documents are not authorized members of that group, their attempts would be tagged and might be blocked, reported to a manager, or protected from modification.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **User Groups** from the **Source/Destination** menu, select **sender is none of** and click **?**.

The directory server pop-up appears.

4 Select a directory server, click **Find** from the **AD pop-up**, and click the process engineers' user group.

5 Click **Apply**.

6 From the **Endpoint** menu, select **Apply Tag Label**, click **?**, and select the appropriate tag from the pop-up.

7 Click **Apply**.

8 From the **Endpoint** menu, select **Tags - Location Path**, click **?**, and use **Find** to select the protected share.

9 Click **Apply**, then **Save**.

Controlling devices

McAfee DLP Endpoint can control any number of devices attached to enterprise managed computers by using device rules to detect, then react to significant events on devices used at network endpoints.

Devices attached to enterprise managed computers — such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or Plug and Play devices — can be monitored or blocked using device rules, allowing you to control their use in the distribution of sensitive information. For example, a global company might use networked McAfee DLP Endpoint to protect sensitive data on USB drives issued by branch offices in other countries — even if the user of that device is on the road.

Device rules monitor and potentially block the system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other Plug and Play devices. They consist of one or more device definitions that can be pre-programmed to affect specific users or a user assignment group. The rule can be used to block, monitor, or send notification when the defined devices are used on- or off-site.

Device rules monitor and potentially block the system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other Plug and Play devices. Device classes and device definitions are used to define device rules.

Role-based device rules can be created for the enterprise workforce. For example, while the majority of workers might not be allowed to run executables from flash drives, IT and sales force might need that privilege to bypass operating systems so they can reformat hard drives.

By using role-based access control with device rules, a variety of users can be monitored or excluded from supervision, securing sensitive data without creating roadblocks to their productivity.

Device classes

Device classes are used to control groups of related devices. Each class of devices is identified by a name, an optional description, and one or more Globally Unique Identifiers (GUIDs). The McAfee DLP client uses the device classes on the **Managed** list to identify devices being used at endpoints.

The device classes on the Managed Device Class list are used by the McAfee DLP client to monitor their usage at endpoints.

If you are using McAfee DLP Endpoint with McAfee DLP Manager, you can find built-in *device classes* listed on the **Device Management** page. The devices are categorized by *status*:

- **Managed** — Specific Plug and Play or removable storage devices, defined by device class, that can be managed by McAfee DLP Endpoint, but whose status can be changed to Unmanaged.
- **Unmanaged** — Device classes not managed by McAfee DLP Endpoint, but whose status can be changed to Managed.
- **Unmanageable** — Device classes not managed by McAfee DLP Endpoint because attempts to manage them might affect the managed computer, system health, or efficiency. New classes of devices cannot be added to this list.

In daily tasks, the system administrator should not tamper with the device classes list because improper use (for example, blocking the managed computer's hard disk controller) can cause a system or operating system malfunction.

Instead of editing an existing item to suit the needs of a device protection rule, add a new, user-defined class to the list.

Classifying devices

Every endpoint device has a unique set of parameters, and device definitions are used to identify each one.

Device parameters, such as Product ID/Vendor ID (PID/VID), or USB class code, are the components of the device definitions. A different set of properties for each device enables blocking or monitoring of specific devices by the system.

Built-in definitions for McAfee Endpoint Encryption for Files and Folders and McAfee Endpoint Encryption for Removable Media facilitate the use of those products with McAfee DLP Endpoint

Defined devices are classified into two groups:

- **Plug and play devices** — Devices that can be added to a managed computer without any configuration or manual installation of dlls and drivers. For example, the system can prevent loading of plug and play devices like Bluetooth, Wi-Fi, and PCMCIA devices. Most Microsoft Windows devices are PnP devices.
- **Removable Storage devices** — Removable external storage devices containing file systems that appear on the managed computer as drives.

While the plug and play device definitions and rules include general device properties, the removable storage device definitions and rules are more flexible and include additional properties related to the removable storage devices. McAfee recommends using the removable storage device definitions and rules to control devices that can be classified as either PnP or removable storage, such as USB mass storage devices.

Whitelisted plug and play devices

Certain plug and play devices are whitelisted because they do not handle device management well, and might cause the system to stop responding or cause other serious problems. McAfee recommends adding such devices to the whitelisted device list to avoid compatibility problems.

Whitelisted plug and play device definitions are added automatically to the **Excluded** list in every plug and play device rule. They are never managed, even if their parent device classes are.

If you inspect the device rules, you do not see the whitelist definition because the definition is not added to the rule until the policy is applied. You do not have to rewrite existing rules to include new whitelisted devices.

Add a new device class

Device classes categorize device types used by the system. Each class of devices is identified by a name, optional description, and one or more Globally Unique Identifiers (GUIDs).

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
   - On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Classes**.

   The available devices appear in the right pane.

3 From an **Actions** menu under **Managed** or **Unmanaged** device classes, select **Add New**.

   A device class window appears.

4 Enter a name, an optional description, and the device's Globally Unique Identifier (GUID).

   A GUID in the correct format is required.

5 Click **Save**.

Change the status of a device class

Devices might be managed, unmanaged, or unmanageable. You can change the status of devices that can be managed or unmanaged.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
   - On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Classes**.

   The available device classes appear.

3 Select a device class checkbox.

4 From the **Actions** menu, select **Mark Status as Managed** or **Mark Status as Unmanaged**.

   If unknown device classes (classes with no name) appear on the dashboard, add them to one of the lists.

Controlling devices with device definitions

Device definitions are collections of parameters that identify managed devices. They are used in device rules to detect significant events on those devices.

When you create a device definition with multiple parameters, each **Parameter Name** is added to the definition as a logical OR, and multiple **Parameter Names** are added as logical ANDs.

For example, the following parameter selection creates the device definition shown below:

Table 13-1 Device definition example

Device definition	Selected parameters
Bus Type	Firewire; USB
Device Class	Memory Devices; Windows Portable Devices

- Bus Type is one of: Firewire (IEEE 1394) *OR* USB
- *AND* Device Class is one of Memory Devices *OR* Windows Portable Devices.

Add a device definition group

Device definition groups can be used to control related devices.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
   - On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**.

   The available devices appear in the right pane.

3 Locate the **Plug and Play Device Definition Group** or **Removable Storage Device Definition Group** section.

   The **Add Plug and Play Device Definition Group** or **Add Removable Storage Device Definition Group** window appears.

4 From the **Actions** menu, select **Add New**.

5 Type in a name and optional description for the new device definition group.

6 From the **Device Definitions** menu, select one or more device definitions from the available list.

7 Click **Save**.

Add a removable storage device definition

Removable storage devices can be identified by the parameters that define them. For example, PCI vendor IDs and USB serial numbers are unique parameters that identify only a single device.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
   - On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**, and locate the **Removable Storage Device Definition** section.

   The available device definitions appear in the right pane.

3 From the **Actions menu**, select **Add New**.

The **Add Removable Storage Device Definition** window appears.

4 Type in a name and optional description.

5 Select a **Parameter Name** checkbox from the available list.

The **Edit Definition Parameter** dialog box appears.

6 Select or enter values that define the parameter.

Click **+** to add additional parameters.

7 Click **Save**.

Add a removable storage file access rule

Removable storage device file access rules are used to block executables on plug-in devices from running. Whitelisted application definitions provide lists of specific files that are exempt from the blocking rule.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**, and locate the **Removable Storage File Access Device Rule** section.

The available device rules appear in the right-hand pane.

3 From the **Actions** menu, select **Add New**.

The **Add Removable Storage File Access Device Rule** window appears.

4 Type in a name and optional description, then select **Active** from the **State** menu.

5 Select the **Include** or **Exclude** checkboxes from the available list to define the device rule.

6 Define the user names, groups, and organizations to whom the device rule will be applied.

Select the **user is none of** condition to exclude any of those parameters.

Click **+** to add additional parameters.

7 Click **Save**.

Add a plug and play device definition

Plug and play device definitions allow you to manage and control most available plug and play devices.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**.

The available device definitions appear.

3 From the **Actions** menu, select **Add New**.

The **Add Plug and Play Device Definition** window appears.

4 Type in a name and optional description for the new device definition.

5 Select a **Parameter Name** checkbox from the available list.

The **Edit Definition Parameter** dialog box appears.

6 Select or enter values that define the parameter.

Click **+** to add additional parameters.

7 Click **Save**.

Add a whitelisted application definition

File access rules prevent users from opening potentially harmful executables from removable storage media. But some applications, such as encryption software, must be whitelisted to exempt them from the blocking rule.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Whitelisted Applications**.

The available whitelisted applications appear.

3 From the **Actions** menu, select **Add New**.

The **Add Whitelisted Applications** window appears.

4 Type the name and file extension of the application to be whitelisted into the **Enter a valid Application Name** box.

5 Click **Add** to add the application to the list.

6 Click **Save**.

Add a whitelisted plug and play definition

Some plug and play devices might cause the system to stop responding or cause other serious problems if they are managed by device control software. McAfee recommends adding such devices to a whitelist to avoid compatibility problems.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions** and scroll down to the **Whitelisted Plug and Play Device Definition** section.

The available definitions appear in the right pane.

3 From the **Actions** menu, select **Add New**.

The **Add Whitelisted Plug and Play Device Definition** window appears.

4 Type in a name and optional description for the definition.

5 Select a **Parameter Name** checkbox from the available list.

The **Edit Definition Parameter** dialog box appears.

6 Select or enter values that define the parameter.

Click **+** to add additional parameters.

7 Click **Save**.

Using device rules

Device rules are made up of *device definitions* and user assignment rules that can be used to control usage of groups of devices. They can be used to trigger actions or use whitelisted application definitions when the devices are used.

Devices attached to enterprise managed computers — such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or Plug and Play devices — can be monitored or blocked using device rules, allowing you to monitor and control their use in the distribution of sensitive information.

Device rules must be activated before they can be used.

Different sets of rules can be devised for the enterprise workforce based on roles and needs. For example, while the majority of workers are not allowed to copy enterprise data to removable storage devices, the IT and sales force can use these devices, and are only monitored by the system. This kind of scenario can be implemented by using the properties of the specific device with a suitable device rule.

Plug and Play and **Removable Storage Device** rules can define a device as **read only**. **Removable Storage File Access** rules might be used to control executables and to include or exclude whitelisted applications.

Types of device rules

Device rules are used to control sensitive data that can be compromised by use of devices at network endpoints.

There are three types of device rule: **Plug and Play**, **removable storage**, and **removable storage file access**.

Plug and play and **removable storage device rules** can be pre-programmed to monitor or block usage of endpoint devices by users, take action when violations occur, and alert other users to those events. **Removable storage device rules** can also prevent data on devices from being appended, modified, or copied. For example, users might be allowed to listen to MP3 players, but their potential use as storage devices can be disallowed.

Removable storage file access rules block executables on plug-in devices from running, and they can also be used to include or exclude whitelisted applications, depending on who is using them. For example, some applications, such as encryption applications on encrypted devices, must be allowed to run, and their executables can be exempted from the blocking rule.

File access rules determine if a file is an executable by its extension. The following extensions are blocked: .bat, .cgi, .cmd, .com, .cpl, .dll, .exe, .jar, .msi, .py, .pyc, .scr, .vb, .vbs, .ws, and .wsf. In addition, files that might be executed from within archives, like .cab, .rar, and .zip files, can also be blocked.

Because block is the only action that is supported by file access rules, there is no need to select actions, as in the other device rules. The file filter driver cannot differentiate between opening and creating an executable; it simply blocks them.

Add a removable storage device rule

Removable storage device rules can be used to block, monitor, and assign read-only and user permissions to external storage devices. Although USB storage devices are Plug and Play as well as removable storage devices, these rules should be used to block their use.

Using a Plug and Play device rule to block a USB storage device can result in blocking the entire USB Hub/Controller. McAfee recommends using removable storage device rules because they allow the device to initialize and register with Windows, and the USB device can also be set to **read only**.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Rules**.

The available rules appear in the right pane.

3 In the **Removable Storage Device Rule** section, select **Add New** from the **Actions** menu.

The **Add Removable Storage Device Rule** window appears.

4 Type in a name and optional description.

5 From the **State** menu, select **Active** to activate the rule.

6 If **Device Definitions** are to be added to the rule, select **Include** or **Exclude** checkboxes to indicate if the devices are to be blocked or encrypted.

7 From the **Actions** menu, select the checkboxes of actions that are to be executed when the rule hits. Each action can be set to execute if the user is on or off the premises, or both.

- Select the **Block** checkbox if the device is to be blocked when the user is on- or offsite, or both.
- Select the **Monitor** checkbox if the device is to be monitored when the user is on- or offsite, or both. If either is selected, select a checkbox that indicates the **Severity** of the violation.
- Select the **Notify User** checkbox if an alert is to be sent when users who are on- or offsite, or both, trigger the **Block** or **Monitor** actions.
- Select the **Read only** checkbox if write access to the device is to be blocked when the user is on- or offsite, or both. This prevents copying to or from the device.

8 Set a **User Assignment** condition if an alert is to be sent to users when the device is used on- or offsite. Users can be identified positively or negatively by name or affiliation, and they can be retrieved from an LDAP server.

Click **+** to add multiple user assignments.

9 Click **Save**.

Add a removable storage file access rule

File access rules control the usage of removable storage devices on the network. They can be used to block or encrypt removable storage devices, prevent applications from being started, or restrict the actions of users.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration.**.
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Rules** and scroll down to the **Removable Storage File Access Rule** section.

The available device management rules appear in the right pane.

3 From the **Actions** menu, select **Add New**.

The **Add Removable Storage File Access Rule** window appears.

4 Type in a name and optional description.

5 From the **State** menu, select **Active** to activate the rule.

6 If **Device Definitions** are to be added to the rule, select **Include** or **Exclude** checkboxes to indicate if the devices are to be blocked or encrypted.

7 If there are applications listed under the **Whitelisted Applications** section, select checkboxes to indicate which ones are to be included or excluded from the rule.

8 Set a **User Assignment** condition if an alert is to be sent to users when the device is used on- or offsite. Users can be identified positively or negatively by name or affiliation, and they can be retrieved from an LDAP server.

Click **+** to add multiple user assignments.

9 Click **Save**.

Add a Plug and Play device rule

Plug and Play device rules can be used to block, monitor, and assign read-only and user permissions to Plug and Play devices. Although USB devices are Plug and Play as well as removable storage devices, the latter should be used to block their use.

Using a Plug and Play rule to block a USB storage device can result in blocking the entire USB Hub/Controller. Plug and Play rules are not very flexible — if a device is blocked, it is completely unavailable for use. It is an "all or nothing" rule; if a device is allowed, it will be completely usable. You cannot block a particular feature of the device or keep the device from performing a particular action.

McAfee recommends using removable storage device rules because they allow the device to initialize and register with Windows, and the USB device can be set to **read only**.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **Endpoint Configuration.**
- On your McAfee DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Rules**.

The available device management rules appear in the right pane.

3 In the **Plug and Play Device Rule** section, select **Add New** from the **Actions** menu.

The **Add Plug and Play Device Rule** window appears.

You can use the Plug and Play device blocking rule to block USB devices, but McAfee recommends using the removable storage device blocking rule instead. Using the Plug and Play device blocking rule can result in blocking the entire USB hub/controller. The removable storage device blocking rule allows the device to initialize and register with the operating system. It also allows you to define the device as read-only.

4 Type in a name and optional description.

5 From the **State** menu, select **Active** to activate the rule.

6 From the **Device Definitions** menu, select device and device group definitions to be added to or excluded from the rule. The **Exclude** option is used to whitelist devices that should not be controlled.

7 From the **Actions** menu, select the checkboxes of actions that are to be executed when the rule hits. Each action can be set to execute if the user is on or off the premises, or both.

Select the **Block** checkbox if the device is to be blocked when the user is on- or offsite, or both.

Select the **Monitor** checkbox if the device is to be monitored when the user is on- or offsite, or both. If either is selected, select a checkbox that indicates the **Severity** of the violation.

Select the **Notify User** checkbox if an alert is to be sent when users who are on- or offsite, or both, trigger the **Block** or **Monitor** actions.

8 Set a **User Assignment** condition if an alert is to be sent to users when the device is used on- or offsite. Users can be identified positively or negatively by name or affiliation, and they can be retrieved from an LDAP server.

Click **+** to add multiple user assignments.

9 Click **Save**.

Device parameters

Device parameters are used to build device definitions, which are incorporated into device rules that secure sensitive data at endpoints.

The following table provides definitions for all parameters used in device definitions.

Device parameters cannot be imported in the McAfee DLP Manager implementation of McAfee DLP Endpoint.

Table 13-2 Device definitions for plug and Play and removable storage devices

Parameter name	Found in...	Description
Bus Type	Both	Selects the device BUS type from the available list (IDE, PCI, and so forth.)
CD/DVD Drives	RS only	A generic category for any CD or DVD drive.

Table 13-2 Device definitions for plug and Play and removable storage devices *(continued)*

Parameter name	Found in...	Description
Content encrypted by McAfee Endpoint Encryption for Files and Folders	RS only	Select to indicate a device protected with McAfee Endpoint Encryption for Files and Folders.
Device Class	PnP only	Selects the device class from the available managed list.
Device Compatible IDs	Both	A list of physical device descriptions. Effective especially with device types other than USB and PCI, which are more easily identified using PCI VendorID/DeviceID or USB PID/VID.
Device Instance ID (Microsoft Windows XP; Microsoft Windows 2000) Device Instance Path (Microsoft Windows Vista; Microsoft Windows 7)	Both	A Windows-generated string that uniquely identifies the device in the system. For example, `USB\VID_0930&PID_6533\5&26450FC&0&6`.
Device Name	Both	The name attached to a hardware device, representing its physical address.
File System Type	RS only	The type of file system, for example NTSF, FAT32, and so forth.
File System Access	RS only	The access to the file system: read only or read-write.
File System Volume Label	RS only	The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.
File System Volume Serial Number	RS only	A 32-bit number generated automatically when a file system is created on the device. It can be viewed by running the command line command `dir x:`, where x: is the drive letter.
PCI VendorID / DeviceID	Both	The PCI VendorID and DeviceID are embedded in the PCI device. These parameters can be obtained from the Hardware ID string of physical devices, for example, `PCI \VEN_8086&DEV_2580&SUBSYS_00000000&REV_04`.
USB Class Code	PnP only	Identifies a physical USB device by its general function. Select the class code from the available list.
USB Device Serial Number	Both	A unique alphanumeric string assigned by the USB device manufacturer, typically for removable storage devices. The serial number is the last part of the instance ID; for example, `USB \VID_3538&PID_0042\00000000002CD8`.A valid serial number must have a minimum of 5 alphanumeric characters and must not contain ampersands (&). If the last part of the instance ID does not follow these requirements, it is not a serial number.
USB Vendor ID / Product ID	Both	The USB VendorID and ProductID are embedded in the USB device. These parameters can be obtained from the Hardware ID string of physical devices, for example: `USB\Vid_3538&Pid_0042`.

Working with endpoint events

Problems identified by the McAfee Agent client might include critical system events, rule violations, administrative events, or events associated with a particular user or device.

For example, outgoing events might be generated when protected data is in motion. They might also include registered and classified content that has been tagged for protection purposes. Disallowed user actions, access violations, or detection of controlled elements might also be reported.

Administrative events reported include notification that McAfee Agent has entered or left bypass mode, or that *Safe Mode* has been detected.

All events and their attributes are displayed on the **Data-in-Use** dashboards on ePolicy Orchestrator or McAfee DLP Manager. Once displayed on the dashboard, they can be filtered by general, administrative, or outgoing conditions.

View endpoint events

You can view events detected by McAfee DLP Endpoint on the McAfee DLP Manager **Data-in-Use** dashboard.

The roles users play in an organization determine what types of events they are allowed to view. If you cannot see them, you might not have the right permissions set. Contact your administrator.

Click the column icon above the dashboard to change the display of event attributes. For example, you might want to display the columns that disclose the origin or destination of an event, its owner, and what activity generated it. By clicking **Details**, you can view more attributes of the event, create a report, or assign it to a case.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select the **Data-in-Use** vector.

The default **Incident Listing** page appears.

3 Click **Details** for more information.

The **Incident Details** page appears.

4 Click any tab on the page to get additional information about the event.

If a document link is available, it will open if the supporting software is installed. If there is another link inside the document, it is likely to be the database object that triggered the incident.

Events reported to McAfee DLP Manager

Specific events are distributed through ePolicy Orchestrator to McAfee DLP Manager dashboards.

Administrative Events

- Agent enters bypass mode
- Agent leaves bypass mode
- User returned from safe mode

Non-administrative Events

- Device plugged in
- Device unplugged
- New device class found
- Network file system protection
- Removable storage protection
- Email protection
- Printing protection
- Network protection
- Device access
- Web post protection
- Application file access protection
- Clipboard protection
- Screen capture protection
- Discovery
- Email Storage Discovery

Typical scenarios

When used with McAfee DLP Manager, McAfee DLP Endpoint can be used to control data at network endpoints. Some typical use cases follow.

Contents

- *Keep data from being copied to removable media*
- *Keep data from being cut and pasted*
- *Protect data with Document Scan Scope*
- *Keep data from being printed to file*
- *Protect data from screen capture*
- *Protect data by identifying text in title bars*
- *Keep data from being printed on network printers*
- *Create user list templates to control access*
- *Keep data from being printed on local printers*
- *Protect data using specific encryption types*

Keep data from being copied to removable media

McAfee DLP Endpoint can be configured to block, monitor, notify, or allow read-only access to removable media. You can combine a **Protect Removable Media** rule with other rule parameters to keep defined data from being copied to one of these devices.

Data that is available through top secret governmental networks relies on the scruples of its users. Using a removable media ensures that secret information cannot be copied and distributed to unauthorized users or organizations.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Keyword** from the **Content** menu and enter an identifying word or phrase into the value field (for example, *Confidential* or *Top Secret*).

If you know the document type, you might want to add another element (for example, **Content Type is any of MS Word**) to identify the content type.

4 From the **Endpoint** menu, select **Protect Removable Media**, click **?**, select the **Enable** checkbox, and click **Apply**.

5 Click the **Actions** tab and click **Add Action**, then select **Removable Media Reaction** from the **Data-in-Use** menu.

6 Review the reaction settings in the **Actions** column.

If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.

You must select at least one **Online** or **Offline** checkbox when you select any action.

7 Click **Save**.

Keep data from being cut and pasted

McAfee DLP Endpoint can be configured to disable clipboard functionality, making it impossible for users to cut or paste data between existing and new documents.

Trusted processes are not part of the clipboard rule logic. Applications with a *Trusted* strategy are not exempt from screen capture rules, and will be blocked like any other application.

For example, if you want to ensure that the contents of financial documents cannot be cut and pasted into new documents, use the *Banking and Financial Sector* with the *Protect Clipboard* rule to protect those documents.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

4 From the **Template** menu, select the *Banking and Financial Sector* document set.

5 Click **Apply**.

6 From the **Endpoint** menu, select **Protect Clipboard**, click **?**, select the **Enable** checkbox, and click **Apply**.

7 Click the **Actions** tab and click **Add Action**, then select **Clipboard Reaction** from the **Data-in-Use** menu.

If you want to add other reactions, such as notifying the owner of the documents or storing evidence of the attempt to copy content, go to the **Action Rules** page, open the **Clipboard Reaction** action rule, and modify it to include those actions.

8 Click **Save**.

Protect data with Document Scan Scope

If you have to find and control documents in which a known word or phrase appears in a specific location in a Microsoft Office document, you can use **Document Scan Scope** to find them quickly and keep them from being distributed.

The **Document Scan Scope** feature allows you to search for strings in the header, footer, and/or body of Microsoft Office documents. This feature improves system performance because the agent need not extract and analyze content from complete documents.

Both network and endpoint applications support document properties, but because **Date Creation** and **Date Modified** are Windows parameters, the network applications do not support those properties.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Add a new policy and rule, or open existing ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 Open the **Content** category, and enter keywords that can be found in the documents you want to protect into the value field, such as *Confidential*.

4 Open the **Endpoint** category and select **Document Scan Scope**.

5 Open the **Source/Destination** category, select **URL** and **is none of**, and enter a name and domain (for example, `yourcompany.com`).

By selecting a negative condition, you exclude that domain, ensuring that documents exchanged legitimately within your company will not be affected — but all others being sent out of your intranet will be processed.

6 Click **?** and select the **Body**, **Footer**, and/or **Header** checkboxes from the **Select items** window.

The keywords you typed in will be matched to those portions of the Microsoft Office document.

7 Click **Apply**.

8 Click the **Action** tab, click **Add Action**, and select an action from the **Data-in-Use** actions.

In this case, you might want to add an **Email** or **WebPost** reaction to block, monitor, and store evidence of the activity, whether they are found online or offline (in computers that are on-site, or disconnected from the network). Those reactions also allow notification and requests for justification, so you might want to modify the rule if those actions are not needed.

9 Click **Save**.

When you check the **Data-in-Use** dashboard, you might find the strings you identified reported as incidents.

Keep data from being printed to file

McAfee DLP Endpoint can be configured to block print functionality that allows printing to the Adobe PDF or Microsoft Image Writer file types. If the **Protect PDF/Image Writers** rule is deployed, McAfee DLP

printer drivers are installed in place of third-party drivers. This prevents users from printing sensitive data to a file.

For example, if you suspect that local users are attempting to print and email corporate confidential documents, you might use the following procedure to detect that activity, extract the content of the document to the evidence server, and notify a manager that the attempt has been made.

McAfee DLP Endpoint uses Microsoft Word and Adobe Reader plug-ins to improve performance.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Template** from the **Content** category menu and click **?**.

The **Templates** pop-up menu appears.

4 From the pop-up menu, select the **Select All** checkbox for **Office Applications** and **Apply**.

5 From the **Source/Destination** menu, select **Email Address** and enter the user's email address in the value field, or select the **Any Email Address** checkbox.

6 From the **Endpoint** menu, select **Protect PDF/Image Writers**, click **?**, select the **Enable** checkbox, and click **Apply**.

7 Click the **Actions** tab and **Add Action**, then select **Printer Reaction** from the **Data-in-Use** menu.

Review the reaction settings in the **Actions** column. If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.

8 Click **Save**.

When an attempt is made to print office documents to common file types, the reaction defined in the action rule will be applied.

Protect data from screen capture

If you want to keep users to record sensitive data by capturing images on a computer, you can configure McAfee DLP Endpoint to disable screen capture functionality.

Trusted processes are not part of the screen capture rule logic. Applications with a *Trusted* strategy are not exempt from screen capture rules, and will be blocked like any other application.

For example, if you want to ensure that engineering drawings cannot be captured, use an *Engineering Drawing and Design Files* template with the *Protect Screen Capture* reaction to protect those proprietary documents.

This procedure describes protection of engineering drawings with a template, but you could get a similar result by adding a screen capture protection rule to the *Registered Engineering Drawings and Design File Violations* rule in the *High Technology Industry IP* policy.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Add a policy and rule to carry and deploy the *Engineering Drawing and Design Files* template.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** page, open the **Content** category.

4 From the **Template** menu, select the *Engineering Drawing and Design Files* document set.

5 From the **Endpoint** category, select **Protect Screen Capture**.

The **Enable** pop-up menu appears.

6 Select the **Enable** checkbox and click **Apply**.

7 Click the **Actions** tab and click **Add Action**, then select the **Print Screen Reaction** from the **Data-in-Use** menu.

If you want to add other reactions, such as notifying the owner of the documents or storing evidence of the attempt to capture content, go to the **Action Rules** page, open the **Print Screen Reaction** action rule, and modify it to include those actions.

8 Click **Save**.

When engineering design documents are detected on a computer, the user will not be able to capture the image.

Protect data by identifying text in title bars

If you want to keep users at endpoints from taking screenshots of specific windows, you can apply a **Protect Screen Capture** parameter to a unified rule.

When text in title bars is used with a **Protect Screen Capture** reaction, the rule is refined by preventing snapshots of windows only if they contain that title.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Open an existing rule that defines data you want to protect, or add a new one.

The **Edit Rule** page appears.

3 From the **Endpoint** category, select **Protect Screen Capture**.

The **Enable** pop-up menu appears.

4 Select the **Enable** checkbox and click **Apply**.

5 From the **Endpoint** category, select **Windows Title** and type the text of the title.

6 Click **Save**.

When the title text is detected on a computer, the user will not be able to capture the image.

Keep data from being printed on network printers

If the **Network Printer** rule is deployed and a directory server is added to McAfee DLP Manager, you can prevent LDAP users from printing sensitive data on network printers.

Before you begin

Some printers cannot be managed in this way, and must be defined on the **Unmanaged Printer Models** page during the **Endpoint Configuration** phase.

For example, if you suspect that network users on- and off-site are attempting to print confidential documents, you might use the following procedure to detect that activity, then notify the user that a company policy against printing confidential documents has been violated and blocked.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Keyword** from the **Content** menu and enter an identifying word or phrase into the value field (for example, *Confidential* or *Top Secret*).

If you know the document type, you might want to add another element (for example, **Content Type is any of MS Word**) to identify the content type.

4 From the **Source/Destination** menu, select **User Groups**, and click **?**.

5 From the directory server pop-up menu, click **Find** and click the appropriate user names, groups, or organizations.

6 Click **Apply**.

7 From the **Endpoint** menu, select **Network Printer**, click **?**, select the **Enable** checkbox, and click **Apply**.

8 Click the **Actions** tab and **Add Action**, then select **Printer Reaction** from the **Data-in-Use** menu.

9 Review the reaction settings in the **Actions** column.

If they do not match your objectives, go to **Action Rules** and edit the action rule, or create a new one.

In this case, you must select the **Online** and **Offline** checkboxes for both **Block** and **Notify** when creating or modifying the action rule.

10 Click **Save**.

When the LDAP users identified try to print documents with the specified keywords on network printers, the actions in the **Network Printer** protection rule will be applied.

Create user list templates to control access

If you want to protect sensitive data from unauthorized users, you can apply user list templates to control access to it.

For example, if you are protecting your source code from off-site employees who are not programmers or developers, you can keep all other users from accessing it by deploying user and source code templates with a rule.

You might use the same list of engineering employees to provide access to functional specifications, design documents, and engineering drawings.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 From the **Actions** menu on the **Templates** page, select **Add Template**.

The **Add Template** page appears.

3 Type in a name for the group of users, and add an optional description.

4 From the **Component Type** menu, select **Source/Destination**.

5 Select **User Groups** and click **?**, and select a directory server.

If you have added a directory server to McAfee DLP Manager, a pop-up menu appears.

6 Click **Find**, select the engineering user group, and click **Apply**.

7 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

8 On the **Add Rule** or **Edit Rule** page, select **Template** from the **Content** category menu and click **?**.

The **Template** pop-up menu appears.

9 Open the **Source Code** category and select checkboxes of the source code type, then click **Apply**.

10 From the **Endpoint** category menu, click **?** and select the template you created for engineering users.

11 Click **Save**.

When the rule matches in network traffic, data repositories, or on endpoints, only authorized users will be allowed to access the source code.

Keep data from being printed on local printers

If the **Protect Local Printers** rule is deployed, McAfee DLP printer drivers are installed in place of third party drivers. This prevents users from printing sensitive data.

For example, if you suspect that local users are attempting to print and email corporate confidential documents, you might use the following procedure to detect that activity, extract the content of the document to the evidence server, and notify a manager that the attempt has been made.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

The **Concepts** pop-up menu appears.

4 From the **Corporate Confidential** menu, select document types or click **Select All**.

5 Click **Apply**.

6 From the **Source/Destination** menu, select **Email Address** and enter the user's email address in the value field, or select the **Any Email Address** checkbox.

7 From the **Endpoint** menu, select **Protect Local Printers**, click **?**, select the **Enable** checkbox, and click **Apply**.

8 Review the reaction settings by clicking the **Actions** tab of the rule to which **Endpoint** parameters have been added.

If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.

9 Click **Save**.

Protect data using specific encryption types

If you suspect that members of your Finance Department are emailing files encrypted with McAfee Endpoint Encryption for PC to their own email accounts so they can work on them at home, you can find them by identifying the encryption type and deploying a protection rule to block that activity.

Encryption types can be used in rules to act on files that are unencrypted, password-protected, or encrypted with a specific algorithm.

If some users are permitted to transmit encrypted files, you can create a **Source/Destination** user exception, or add a **Request Justification** option to the reaction.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

The **Concepts** pop-up menu appears.

4 From the **Corporate Confidential** menu, select document types or click **Select All**.

5 Click **Apply**.

6 From the **Source/Destination** menu, select **User Groups**, and click **?**.

7 From the directory server pop-up menu, click **Find** and select the Finance Department group.

8 Click **Apply**.

9 If you want to define a user exception, add another **Source/Destination** parameter.

For example, you might select a **User Name** from the directory server and add a **sender is none of** condition. Alternatively, you might enter the email address of the authorized user into the value field and accept the default **sender is any of** condition.

10 From the **Endpoint** menu, select **Encryption Types** and click **?**.

11 Select the **McAfee Endpoint Encryption for PC** checkbox and click **Apply**.

12 Click the **Actions** tab, click **Add Action**, and select **Email Reaction**.

13 Review the settings in the **Actions** column.

If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.

14 Click **Save**.

When the defined encryption type is detected, the **Email Reaction** protection rule will fire and prevent the transmission of encrypted data.

14 Scanning databases and file repositories

McAfee DLP Discover scans file systems, databases, and endpoints to identify and protect sensitive data at rest in file systems or databases. When incidents or events are reported, they can be automatically protected by moving, copying, encrypting, or deleting unstructured data that might compromise the security of the repository.

Contents

- *Types of scans*
- *Scanning databases*
- *Scanning file repositories*
- *Registering documents and structured data*
- *Managing scans*
- *Managing discovered files*
- *Scan statistics and reports*
- *Typical scenarios*

Types of scans

McAfee DLP Discover scan types support inventory, registration, discovery, and classification of sensitive data. These four scan types are used to crawl network file systems or database repositories.

Table 14-1 Types of scans

Scan type	Description
Classification scan	Helps you understand of the type of data that exists in the targeted repository. McAfee DLP Discover sorts scanned data into different content types and analyzes attributes such as file size, location, type, and concepts. Scanned content is evaluated against policies and rules, allowing you to create optimized Registration or Discover scans. Classification scans cannot be performed on database repositories.
Inventory scan	Allows you to see what needs protection before running a Registration or Discover scan. Use this scan to crawl all directories and files residing on a targeted repository and generate an index, or manifest. For databases, an Inventory scan produces a schema, which consists of the database structure and number of records. Files and database records are not fetched — only metadata is collected. Files are classified based on file extension.

Table 14-1 Types of scans *(continued)*

Scan type	Description
Registration scan	Registers sensitive data by generating digital fingerprints, or signatures, that identify the documents to protect. You can register partial documents by defining excluded text within the documents. For database scans, this is known as **Data Match**. When scanning large databases, McAfee recommends registering only sensitive data, such as bank account numbers or social security numbers. Registering an entire database is not practical or useful.
Discover scan	Finds data that has been registered or data residing on a file share that is in violation of a policy. McAfee DLP Discover can monitor, encrypt, copy, delete, or move files to an export location. All actions produce incidents that are reported to dashboards. You can sort, filter, export, and save remediated incidents to prevent future violations. Remediation actions cannot be performed on database repositories.

Supported repositories with McAfee DLP Discover

McAfee DLP Discover supports several common database repositories, file systems, and servers.

Table 14-2 Supported repositories

Database repositories	File systems and servers

• DB2 — 5x iSeries, 6.1 iSeries, 7.x–9.x
• Microsoft SQL Server 2000, 2005, 2008, 7.0, MSDE 2000
• MySQL (Enterprise) 5.0.x, 5.1
• Oracle 8i, 9i, 10g, 11g
	• EMC Celerra 5.6
	• EMC Documentum 5.3, 6.0, 6.5
	• Microsoft SharePoint 2007, 2010
	• FTP
	• HTTP/HTTPS
	• NFS (Network File System)
	• CIFS (Common Internet File System)
	  • Microsoft Windows Server 2003, 2008, 2008 R2 cluster
	  • Microsoft Windows XP Professional SP3 or later (32-bit)
	  • Microsoft Windows Vista SP1 or later Enterprise and Business editions (32-bit)
	  • Microsoft Windows 7 SP1 or later (32- and 64-bit)
	  • NetApp 7.2, 7.3

Scanning network attached storage

McAfee DLP Discover scans storage devices by using the protocols that are used to access them.

Table 14-3 Common network storage types

Storage type	Access method
Network Attached Storage	Network Attached Storage presents a conventional file system to the network, and can be accessed directly by McAfee DLP systems.
Storage Area Networks	Store data in an unusable format using physical blocks of disk space, but McAfee DLP Discover can connect through any server that owns a pool of data on that device.

Firewall options for scanning

Before scanning a repository, any intermediary firewalls must be configured to allow scans.

Source ports are randomly chosen unless explicitly noted. Network and host-based firewalls typically permit connections only on certain ports and might have to be configured to permit connections on other ports.

Table 14-4 Firewall options

Repository type	Direction	Ports
CIFS	Discover to Server	TCP 139 and 445 on server
FTP Active Mode (tried by Discover if Passive Mode fails)	Discover to Server	TCP destination port 21 on server (control)
FTP Active Mode	Server to Discover	TCP source port 20 (from server), and destination port (on Discover) chosen by Discover (data)
FTP Passive Mode (tried first by Discover)	Discover to Server	TCP destination port 21 on server (control), and another port on server (data) chosen by the server
HTTP	Discover to Server	TCP destination port 80 on server, unless port is manually configured in the URL itself
HTTPS	Discover to Server	TCP destination port 443 on server, unless port is manually configured in the URL itself
NFS	Discover to Server	TCP and UDP destination ports 111; 2049 on server
Database	Discover to Server	Standard ports, by database: • DB2 — 50000 • Microsoft SQL — 1433 • MySQL — 3306 • Oracle — 1521 If the database server is running on a non-standard port, that port number must be punctured in a firewall.
EMC Documentum	Discover to Server	TCP destination port 1489 on server
Microsoft SharePoint	Discover to Server	TCP destination ports 80 (HTTP) or 443 (HTTPS) on server, unless port is manually configured in the URL itself

Scanning databases

Dynamic Data Registration, also known as **DBReg**, is a method of fingerprinting large volumes of data using the **Data Match** function. The type of data registered might include extended caches of customer names and account numbers, credit card numbers, patient records, or any other type of structured data.

Up to 300 million records can be registered and tracked as they are moved. In addition, data that has been identified can be associated with a rule to provide long-term protection.

The data retrieved using this method matches specific data values, not just patterns that describe the data, and fine distinctions can be made between matches. For example, customer credit card numbers might be reported as privacy violations, but an employee's own credit card number can be defined as an exception and ignored.

The same mechanisms that support registration of flat files also support registration of database records. For example, the signatures produced by data matching are stored in a factory default concept, **DBReg**, which collects structured data in the form of comma-separated values of exported columns (fields) found in databases.

The **DocReg** concept performs the same function for documents.

Database terminology

Terminology that identifies database properties is determined by database types, which vary by vendor. McAfee DLP Discover uses the appropriate object hierarchy when setting up filtering options for scans.

The object hierarchy used by the supported database types varies. The five filtering components supported by McAfee DLP Discover are catalogs, schemas, tables, columns, and records and rows.

Schemas are collections of database objects that are owned or have been created by a particular user, and catalogs are collections of related schemas.

But these terms are used interchangeably in MySQL databases, and Microsoft SQL Server defines a catalog/schema model for data stores. In this model, catalogs contain schemas. By contrast, Oracle and DB2 database use only the term schemas.

Whether the term schema or catalog is used, all databases contain tables, which contain records and rows. McAfee DLP Discover database scanning extends to the records and rows level.

How database content is registered

Database content is registered by uploading structured data, scanning a database, or deploying rules that identify sensitive data during the discovery process.

You can use McAfee DLP Discover to register database content using one of three methods.

- Upload data in structured format on the **Web Upload** page.
- Create a Registration database scan on the **Scan Operations** page
- Embed the DBReg attribute in one or more rules on the **Edit Rule** page.

Register structured data by uploading

Register structured data found in a database by uploading it to McAfee DLP Discover. You can use the registered objects to detect similar content in other repositories.

If you use McAfee DLP Manager to upload structured data, it will automatically be registered on all managed devices.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **Policies** | **Registered Documents** | **Data Registration**.
   - On your McAfee DLP appliance, select **Policies** | **Registered Documents** | **Data Registration**.

2 In the **Actions** tab, select **Upload New File**.

3 Click **Browse** to locate the data that needs protection.

Data must be in CSV (comma-separate values) format.

You can upload large CSV files by compressing them into a single ZIP archive.

4 Type in a file name.

The **Signature Type** field defaults to **High Granularity**, which is the only choice for documents that are registered by uploading.

5 From the **Policy** menu, select a policy.

6 From the **Rule** menu, select a rule.

The rules listed are the only ones available, because they are the components of the selected policy.

7 From the **Devices** box, select the device that will receive the uploaded data.

8 Click **Save** or **Save & Upload Another**.

Database filtering options

The hierarchical structure of the targeted database determines the filtering options available.

Table 14-5 Filtering options by database type

Database type	Filtering options
MySQL	Catalogs, tables, columns, records/rows
Oracle	Schemas, tables, columns, records/rows Built-in schemas for Oracle, such as SYSTEM, SYS, XDB, TSMSYS, and WMSYS are ignored during a database crawl.
DB2	Schemas, tables, columns, records/rows
MS SQL Server	Catalogs, schemas, tables, columns, records/rows

Defining the database to be scanned

Before a database can be scanned, its host name or IP address must be defined to identify the targeted repository.

When you have completed the node entries, click **Include**. You can also **Test** the database connection.

Table 14-6 Node definition settings for database scans

Option	Definition
IP Address	Host names or single IP Addresses are allowed. For Oracle Real Application Clusters, use the VIP (virtual IP address) of node1 (or node2 of RAC) For MS SQL Server databases with multiple instances, use `<host ip>\\<db instance name>` (for example, `172.20.242.151\\N14N`).
Port	Ports are automatically configured, according to the database type: • DB2 — 50000 • Microsoft Server — 1433 • MySQL — 3306 • Oracle — 1521 Enter non-standard ports in the text box.
SID	For Oracle RAC, use the service name of the RAC.
Login Database	Type the name of the login database. For SQL, this is the database instance. For Oracle, use the SID (System ID).
SSL Certificate	Certificates are created and saved on the Discover configuration **SSL Certificates** page. Click **New** to create a new certificate, or use an existing one. Use the **ANY** SSL option if you want McAfee DLP Discover to accept any SSL certificate. McAfee DLP Discover will not verify authenticity of presented certificates, but data connections will be encrypted.

Catalog options for database scans

Catalog options are available for use in SQL database scans.

Table 14-7 Catalog options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the catalog name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the catalog name entered in the VALUE parameter.

Schema options for database scans

Schema options are available for use in all types of database scans except for MySQL.

Table 14-8 Schema options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the schema name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the schema name entered in the VALUE parameter.

Table options for database scans

Table options are available for use in all types of database scans.

Table 14-9 Table options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the table name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the table name entered in the VALUE parameter.

Column options for database scans

Column options are available for use in all types of database scans.

Table 14-10 Column options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the column name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the column name entered in the VALUE parameter.

Record and row options for database scans

Database scans can be run on a specified number of records or rows, allowing definition of a very narrow range of data. In SQL databases, patterning can be used to retrieve specific results from columns.

Table 14-11 Record and row options for database scans

Option	Definition
Where	Allows entry of any SQL **where** clause. For example, retrieve matching names from columns in a table by entering surnames like `'%lang';` . The **where** clause will be used as standard SQL and appended while scanning the table. If the column(s) specified here are not indexed or contain large textual data, the performance of the crawl can be affected, and might also impact other clients connected to the database.
Limit (number of rows)	Limits the number of rows fetched from each table. If you set a limit of 100, it means at most one hundred rows will be fetched from each table crawled.

Setting conditions in database scans

When a scan task is set up, conditions are used to constrain the scan to a specific portion of the database component being filtered.

For example, McAfee DLP Discover might be configured to crawl all columns and rows of one table in a single schema of an MS SQL catalog. Such a configuration might be useful for finding all employees in a group under a single department manager of a business unit.

Set the conditions in the **Filters** tab on the **Add Scan Operation** page.

Logon options for database scans

Logons authenticate users to the databases to be scanned, and options vary according to database type.

Table 14-12 Logon options for database scans

Option	Definition
Login	• For SQL databases, use the database instance. • For Oracle databases, use the System ID.

Port options for database scans

Port numbers for each of the database types are already set. If a different port is to be used for the scan, it can be defined in the **Node Definition** tab.

Table 14-13 Port options for database scans

Option	Definition
Port	Ports are automatically configured according to database type. Enter non-standard ports in the Node Definition **Port** box. • DB2 - 50000 • Microsoft SQL Server - 1433 • MySQL - 3306 • Oracle - 1521

Advanced options for database scans

McAfee DLP Discover supports configuration of bandwidth and email notification in addition to routine scanning tasks. These options are available on the **Add Scan Operation** page in the **Advanced Options** tab.

Bandwidth throttling allows you to set a specific data transfer rate for a scan. Email notification allows set up of notification when a scan has started, stopped or both.

Email subject fields are not customizable. There might be a lag of a few minutes between the actual task start-stop time and the email posting. The end notification is sent at the end of scanning. Records processing might continue after notification.

Table 14-14 Schema options for database scans

Option	Definition
Bandwidth	When throttling is activated, allows users to set bandwidth allocated to a scan.
Email Notification	Notifies users of scanning operations if **On Start** or **On End** is selected.
Email To / On Start	Sends customized email to a user when a scan starts.
Email To / On End	Sends customized email to a user when a scan is complete.

Using SSL certificates

SSL certificates are used to authenticate and encrypt connections.

By default, database scans that are configured to use SSL certificates enforce host name verification when negotiating an SSL connection with the database server. This ensures that the host name in the certificate matches the host name defined in the scan URL, which helps prevent man-in-the-middle attacks.

In some situations, the host name in the SSL certificate might differ from the host name of the database server. For example, the certificate is configured to use *xyz.example.net*, but the host name specified in the scan URL is *xyz1.example.net*. In these situations, the SSL connection will fail. Host name verification can not be disabled. If the certificate and scan URL host names do not match, consider these options:

- When configuring the scan, specify the host name as it appears in the SSL certificate that the database server presents. Verify that DNS resolves correctly.
- Configure the SSL certificate of the database server to use the correct host name.
- Configure the McAfee DLP Discover scan to accept any SSL certificate.

SSL certificate settings

SSL certificates identify the database server host and encrypt the data exchanged between database server and the McAfee DLP device.

Databases must be set up to allow the McAfee DLP Discover client to connect using an SSL socket.

All of the database types different configuration requirements for SSL, and if a certificate is required, it must be exported from the server that is to be scanned. The services of a database administrator will be needed to handle these tasks.

McAfee DLP Discover client certificate handling is currently not supported.

After the certificate is exported, it is imported into the TrustStore of the McAfee DLP Discover appliance.

Table 14-15 SSL certificate settings for database scans

Option	Definition
No SSL Certificate	The database does not require a certificate, or the data transfer does not need to be encrypted.
Any SSL certificate	A certificate is required, but it can be non-standard or self-signed.
Signed SSL certificate	The certificate must be verified by a legitimate authority.

Add an SSL certificate

If a secure channel is needed for a database crawl, an SSL certificate might be used to encrypt traffic between the repository and the McAfee DLP Discover client.

If a certificate is to be used, the Database Administrator of the targeted repository must first configure the database to use SSL for authentication and data exchange with clients. This involves exporting the public key of the SSL certificate to a file that the McAfee DLP administrator will downloads for later upload to McAfee DLP Discover.

DBAs should refer to the appropriate database user manual for details. The certificate must be PEM/X.509 standard, and in one of two formats: .cer (Base64 encoded) or .der (Windows encoded).

This procedure explains only the SSL certificate portion of the creation of a database scan. When this part of the process is complete, the SSL certificate will have been uploaded to the McAfee DLP Discover appliance.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **SSL Certificates**.
   - On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **SSL Certificates**.

2 Select **Actions** | **New**.

3 Type in a name and optional description for the certificate.

4 Browse to the location of the certificate on your desktop.

Click the magnifying glass icon to get **Certificate Details** before you save it.

If the certificate hasn't yet been exported from the repository to be scanned, contact the database administrator.

5 Type in the **Host Name** or IP address of the database server.

6 Click **Save**.

The certificate be uploaded to the McAfee DLP Discover appliance and stored in the TrustStore of the database crawler, and its identifying characteristics will appear in the **Edit SSL Certificate** window.

After you have added the certificate and saved the task, you can start it. If the certificate matches the exported from the database, the crawler will start.

Troubleshooting the SSL certificate

If the crawl fails to validate the certificate, you can log on as root to the McAfee DLP Discover appliance to examine the certificates in the TrustStore.

Change directory to `/data/stingray/python`, then view the contents of the certificate file by running this command:

```
# ./certificate_ct1.py LIST
```

You can match up the information in this file to the **Certificate Details** pane of the **Edit SSL Certificate** window.

Scanning file repositories

The **Data Classification** feature sorts crawled data into different content types and evalutes the likelihood of potential rule violations before they are reported. That knowledge can be used to create new protection strategies and optimized, more effective scans.

This feature is not available for database scanning, but you can create an inventory scan for the database to estimate the size and its schema structure.

Without enough information about the characteristics of data in a repository, constructing a protection strategy for the data involves trial and error. Sensitive data might be sampled with different types of crawls, and trial runs might be done using different combinations of rules and policies.

Data Classification uses an OLAP data model to obviate the need for such time-consuming tactics, producing comprehensive and useful information so that new strategies can be devised and significant results can be retrieved more quickly.

Once data has been classified for use in optimized scans, OLAP tools can be used to manipulate and record it.

How McAfee DLP Discover uses OLAP

McAfee DLP Discover databases are configured to use *Online Analytical Processing*, a data model that enables processing of metadata at rapid rates from many different viewpoints. The process creates multidimensional relationships between data values.

When McAfee DLP Discover scans a file system repository, each value, or *hypercube*, is compared to many others in the database. A web of relationships between data values produces previously unknown data patterns that can be used to protect data at rest quickly and more effectively.

When an optimized Discover scan is run after data has been classified and stored in a multidimensional OLAP database, new knowledge about the data can be used to estimate potential violations. Using data that describes the context of data values amplifies its usabilty and extends the effectiveness of discovery.

McAfee DLP Discover includes OLAP tools that enable users to explore all aspects of the scanned data. Evaluating the contents of a repository or share before scanning makes it possible to invent new protection strategies that will focus efforts more precisely on data at risk.

The OLAP Navigator

The **OLAP Navigator** displayed on the **Predefined View** and **Task View** pages provides tools that allow users to manipulate classified data.

The OLAP tools give you the ability to explore, drill down, chart, print and report classified data in an infinite number of configurations.

You must be authorized to view **Data Classification** results. An administrator must add that privilege to your user group under **Discover Scan Permissions**.

Each of the attributes listed under **Columns** and **Rows** offer an opportunity to explore the classified data produced by the scan you are analyzing.

After you have analyzed a view, you can clear it by clicking **X**.

Table 14-16 OLAP tools

OLAP tool	Function
OLAP Navigator	Displays potential rule hits using the classified data available for each.
Drill position	Offers the ability to drill down to finer granualarity data levels by clicking **+**.
Show/Hide Chart	Use the values to show or hide the default chart.
Chart Configuration	Use chart settings to create a new chart.
Configure Print Settings	Use print settings to print a new chart.
Print to PDF	Save the results in a PDF report.
Export to Excel	Save the results in a CSV report.

How the classification engine works

The data classification engine operates on two levels: during scan operations, and on the McAfee DLP device.

When inventory and classification scans run, the classification engine crawls the defined repository, reports the files and directory attributes (file name, size, path, etc.) found at that location, classifies them by file type, and reports the results in a several different predefined views.

During a classification scan, the inventory phase is followed by fetching and classifying the content that is found in the repository. The classification engine then stores the existing information about the data (metadata) in a classification database, and it is available on the **Data Classification** dashboard.

The data can then be used to add refined Discover and Registration scans that allow targeting of specific content types and policies.

Classification scans do not generate incidents on **Data-at-Rest** dashboards.

How data classification scans work

Data classification scans can be used as an interim step between Inventory and Discover scans. They build on inventoried data, classifying it by content type and predicting the type of violations that are likely to be found in the repository.

When the results of a classification scan are used as a starting point for new scans, investigation of a repository returns multidimensional results that offer users more ways to protect data and better results.

Classification scans are especially useful because of their speed and flexibliity. Manifests of file systems produced by Inventory scans are made up of long lists of data that is difficult and time-consuming to analyze. Doing full Discover scans of large repositories might produce so much data that significant patterns might go unrecognized, and the lack of information about the data might lead to incorrect protection strategies.

Classification scans run after repository data has been indexed and before incidents are discovered. This interim step reduces overhead of the scan on the targeted server while increasing the value of reported results.

Currently, the **Data Classification** feature supports only file-based scans (CIFS, NFS, HTTP, HTTPS, FTP, Documentum, and SharePoint).

How categories are used to forecast rule hits

Categories displayed on the **Task View** page contain rules that could potentially be violated if a Discover scan were run on that share or repository. By exploring each available option, you can figure out what combination of scan parameters will give you the best results.

Other attributes include the share, file types, and owners of the classified data. The **Measures** attributes include the number and size of the files that might be discovered.

Data classification workflow

The **Data Classification** workflow objective is to prepare data found on a repository for optimized scans that can produce significant results quickly.

After you create a classification scan that crawls a specified repository, the classification engine sorts the scanned data and displays it in graphical form on the **Data Classification** page.

Data displayed in the **Predefined View** is made up of any classified data resulting from all scans performed on the McAfee DLP Discover appliance.

Data displayed in the **Task View** is made up of any classified data resulting from a single scan performed by the McAfee DLP Discover appliance. In this view, the sorted data is available for use in subsequent scans by content type (and in the case of a Discover scan, by policy), making it possible to create a refined scan that runs on a very narrow range of data.

How classified data is displayed

Classified data is displayed in two different views. **Predefined Views** can be used for common scenarios, and **Task Views** are user-configurable.

The **Predefined View** is at the McAfee DLP device level, and shows all possible data that has been collected by various scans. The **Task View** is at scan task level, and shows data that has been collected by specific scan operations.

In the **Predefined View** , you can use the **OLAP Navigator** to review many different aspects of the classified data. You can examine discovered data in graphical format, export to a report, or save to a CSV file format.

The results on the **Predefined** dashboard contain all possible data that has been collected by varous scans in a variety of formats, and they are displayed in ways that many users will find helpful. These useful views are provided for user convenience.

In the **Task View**, you see a list of all scans that are doing classification. You can click the **Analysis** icon to find the data classified by that scan, then select aspects of it that can be used in additional scans.

As in the **Predefined View**, when you see the data from those scans in the **Task View**, you can graph, export, or save them to a CSV file format.

Depending on the number of variables, some of the text along the x-axis might not be visible in the expanded chart. Use the tabular view to display the full text.

Predefined views of classified data

The **Predefined View** is device-based. It contains classified data gathered from all McAfee DLP Discover devices on the network that have stored results of multiple scans.

These contextual views display classified data in a variety of formats.

Table 14-17 Device data classification views

Device context view type	Data types displayed
Global	Dimensions such as device, task, repository, share and file type
Repository-Share-File Type view	Repository, share and file type
Device-File Type view	Device and file type
Device-Task-File Type view	Device, task and file type
Task-File Type view	Task and file type
File Type-Repository-Share view	Type and repository
File Type-Device view	Type and device
Category-Owner view	Category and owner
Category-Repository view	Repository
Category-Repository-Share view	Repository and share
File Type-Share view	File type and share
File Type-Owner view	File type and owner

Task view of classified data

The **Task View** page lists all classified and inventory scans. **Statistics** and **Analysis** options are available for each scan.

Selecting **Statistics** on the **Task View** page opens the **Scan Statistics** page. The results of the scan are displayed in the same way as scans that do not create classified content.

Selecting **Analysis** on the **Task View** page opens the **Data Classification** page for that scan. The results of that scan are not only displayed as statistics, but they are also highly configurable. The OLAP tools offer exploration, drill-down, charting, printing and reporting options.

Creating optimized scans from the Task View page

After a classification scan is defined, an optimized scan can be created from the **Task View** page. All of the values defined in the classification scan populate matching fields in the optimized scan.

Even after values from the **Select Classified Data** menu are applied to an optimized scan, it can still be edited on the **Edit Scan Operation** page. The existing applied filters can be used or excluded as needed.

Create an optimized scan from classified data

When you evaluate classified data before creating a new scan, you can refine scan filters to produce more effective results.

Before you begin

Create and run a data classification scan to provide content and context for the optimized scan.

Task

1. Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Data Classification**.
   - On your McAfee DLP appliance, select **Classify** | **Data Classification**.
2. On the **Task View** page, select an Inventory or Classification scan that might have the type of classified data you need to get optimized results.
3. Click the **Analysis** icon of the selected scan.

   A page of sorted and configurable results appears.
4. From the drop-down list, select a scan mode.
5. Click **Create Task**.

   The **Select Classified Data** window appears.
6. Select the file extensions to define the classified content, then select the shares you want to scan.

   If you are creating a Discover scan, you must also select one or more policies to indicate what rules you want to match to the classified data.
7. Click **Generate**.

   The **Add Scan Operation** page appears.
8. Click the **Policies** and **Filters** tabs to verify the new options in the scan definition.
9. Click **Save**.

Registering documents and structured data

Data in documents and databases can be registered by uploading files or structured data or by using a Registration scan to create signatures for many files in a defined location. You can also register files using a McAfee DLP Discover scan to match rules to data at rest to tag sensitive data, embed signatures in rules that run on a regular basis, or deploy signatures to endpoints through McAfee DLP Agent.

Signatures that identify registered data are stored in two factory default concepts:

- **DocReg** — Document registration for unstructured data
- **DBReg** — Data registration for structured data

The content of these two concepts can be accessed by adding them as components to rules that are used to crawl repositories during a Discover scan.

For McAfee DLP Endpoint scans, the signatures are stored in registered document packages that are deployed to endpoints.

When data is registered by the web upload method, all devices registered to McAfee DLP Manager at that time will receive the signatures. When data is registered by scanning, you can choose the device that will store the signatures.

There are four ways to register content:

- Uploading files or structured data
- Applying policies to data at rest in repositories
- Using signature collections (DocReg or DBReg) or signatures created with a SHA-2 sum utility in rules
- Scanning endpoints and deploying the signature package to McAfee DLP Agent

Signatures that identify sensitive data are generated by complex algorithms during a registration scan or by uploading documents. Each protected document might contain hundreds of overlapping signatures, which are expressed as hexadecimal numbers. The density, or fidelity, of the signature tiling depends on the level of detection needed.

Typically, the registration process runs whenever a document is uploaded to a McAfee DLP Discover appliance, or when a Registration scan runs on a designated file system or database.

Types of signatures

The signature type selected when data is registered determines the density of signatures generated during registration.

Signature types vary depending on usage and available memory.

When registered text is plagiarized, it is unlikely that a 100 percent match will be found to the original document. Therefore, searching for a percentage match of the registered material is more likely to expose intellectual property theft.

Use the high granularity signature type to detect percentages of matching signatures.

Signatures are not created for empty files.

Table 14-18 Definitions of signature types

Signature type	Definition
High granularity	Full plagiarism detection and protection by generating overlapping tiles over every bit of text. The original document can be identified, even if words are transposed or the contents differ by a couple of lines of text. Only high granularity signature types are generated for Web Uploaded documents.
Medium granularity	Basic plagiarism detection and protection by generating tiles over every eighth word. The original document can be identified even if the contents differ by a couple of pages of text.
Low granularity	Single, compact digital signature for each document registered. Exact copies of the file can be detected.

How signatures are shared with managed systems

Managed McAfee DLP Discover appliances automatically send signatures generated from scans or web uploads to McAfee DLP Manager.

McAfee DLP Manager can send these signatures to any managed McAfee DLP device. Use the DocReg or DBReg concepts in a rule to allow other McAfee DLP devices to perform signature matching on files and data.

McAfee DLP supports up to 1.8 GB of space for DocReg signatures and up to 1.2 GB of space for DBReg signatures.

Add DocReg or DBReg to a rule

Add the *DocReg* or *DBReg* concepts to a rule to match signatures to data at rest in file systems and database repositories.

You can add up to two scan tasks to a rule, but only one of each type (**Data-in-Motion** or **Data at Rest**). The definition of the rule determines which type is targeted.

If you add a scan task to a rule after the *DocReg* or *DBReg* concept is added, you can apply existing signatures to the data that was registered or discovered by that task.

If a Registration task is used with the *DocReg* or *DBReg* concepts, the rule will also be evaluated by any Discover scan that uses its policy. You must manually configure the rule to include the concept if you want to register the same document across multiple rules.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Select a policy, then click a rule.

3 Select the **Content** category.

4 Click **+** to add an element.

5 Select **Concept is any of**.

6 Click **?**, open **Corporate Confidential**, and select **DocReg** or **DBReg**.

This instructs the rule to match all existing signatures to the content you defined.

7 Click **Save**.

Alternatively, click **Save as Rule** to open a rule definition page. Adding this rule to a policy allows you to use the **DBReg** or **DocReg** concepts to identify sensitive data automatically whenever that policy is used to find incidents.

Examples

If **DocReg** is added to the *PII Social Security Number in Documents*, it will find signatures only in stationary documents.

If **DBReg** is added to *Social Security Number in Email and Instant Messaging Conversations*, it will find signatures only in streaming network data.

Upload documents and data for registration

Register documents and data in repositories by uploading files to your McAfee DLP appliance. If they are registered through McAfee DLP Manager, the files will automatically be registered on all managed devices.

Before you begin

- Document files cannot be over 10 MB.
- Data files cannot be over 100 MB. Data in repositories must be uploaded in a comma-separated values (CSV) file. You can compress the file in a format such as ZIP or TAR before uploading, but the compressed file must also be under 100 MB. There are no size limits on files after they are uploaded and decompressed.

Role-based access control determines which users are able to register data.

When uploading documents or data, you do not need to define the McAfee DLP device that stores the file. All devices are automatically selected by default.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Registered Documents**.
- On your McAfee DLP appliance, select **Policies** | **Registered Documents**.

2 Select one of these options:

- For DocReg (document registration), select **Web Upload**.
- For DBReg (data registration), select **Data Registration**.

3 From the **Actions** menu, select **Upload New File**.

4 Browse to the file you want to register.

5 Select the policy and rule you want to use to detect the document.

For example, if your goal is to protect design documents, you might select the *High Technology Industry IP* policy and the *Design Documents Emailed to Competition* rule.

6 Click **Save**, or **Save, Upload Another**.

When you click **Save**, the signature of the document is added to the **DocReg** concept. All web uploaded documents are collected in that concept; they are treated as a group, not registered individually.

Document registration queries the browser for the local path of the file on the client machine. This information is used for easy recall in later uploads. However, some browsers might present a security warning about this. You can choose to disallow sending the local file path. The file will still upload, but the local path might not be recorded on the McAfee DLP appliance.

Reconfigure Firefox 3.5.x to view complete paths

Firefox 3.5.x does not display complete paths for security reasons. If you use this browser, it can be configured to view complete paths when a file is discovered.

Other browsers might also provide security alerts when uploading files. Reconfigure these browsers appropriately if needed.

Task

1 Enter `about:config` in the Firefox address bar.

Click the button acknowledging the warning.

2 Double-click `signed.applets.codebase_principal_support`.

3 Close and re-open Firefox.

4 Upload a file.

5 Click **Allow** on the **Internet Security** pop-up window.

Exclude text from registration

Exclude text from registration to improve performance and clear the dashboard for significant results. Text that is excluded might include boilerplates files or other innocuous content.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Registered Documents** | **Excluded Text**.
- On your McAfee DLP appliance, select **Policies** | **Registered Documents** | **Excluded Text**.

2 From the **Actions** menu, select **New Text**.

3 Open the document containing the text to be excluded.

4 Cut and paste the text into the **Text to Exclude** box.

5 Click **Save**.

Unregister content

You can Unregister content that is not relevant to your results.

There is a limitation on the number of files that can be unregistered. If you have a large number of files to unregister, consider creating a new scan with a smaller scope and appropriate filters.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Registered Documents** | **Data Registration**.
- On your McAfee DLP appliance, select **Policies** | **Registered Documents** | **Data Registration**.

2 From the **Actions** menu, select **Unregister**.

When this is done, the registration crawler will exclude the document or data from future registration.

Re-register content

Re-register content that has been unregistered.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Registered Documents** | **Data Registration**.
- On your McAfee DLP appliance, select **Policies** | **Registered Documents** | **Data Registration**.

2 From the **Actions** menu, select **Reregister**.

The registration crawler will restore the document or data from future registration.

Managing scans

Scan operations are managed by applying different states from the **Actions** menu on the **Scan Operations** page.

Scan operations can be paused and resumed, and notification can be set up to inform users that a crawl has started and stopped.

Table 14-19 Scan actions

Scan action	Description
New	Opens the **Add Scan Operation** dialog box.
Clone	Copies the selected scan and opens the **Edit Scan Operation** dialog box; allows name and other parameters to be changed.
Activate	Activates the selected scan, which scan is enabled to run (on schedule). Only active scans are allowed to be run. Activation causes system to fetch files and analyze content.
Deactivate	Deactivates the selected scan (keeps it from running).
Start	Starts the scan.
Stop	Stops the scan.
Abort	Stops the scan abruptly without processing the fetched files.
Rescan	Resubmits the scan for tasks that are not running, but are in a Ready state; re-fetches files and re-analyzes all content, and generates new incidents.
Delete	Deletes the scan.

Preparing to scan

Before creating a scan, create a framework for your protection strategy by considering the following parameters:

- Scan mode (Inventory, Registration, Discover or Classification)
- Credentials to access the repository
- Database type and version (for database scans)
- IP address, subnet, or range of the targeted repositories, including required ports
- Login database or SID and SSL certificate (for database scans)
- File systems to be scanned

- Schedule for the scan
- Configuration of firewalls
- Bandwidth to be used
- Projected scan load

Configuring Microsoft SharePoint scans

When setting up a SharePoint scan — or *crawl* — consider these points.

- If a full page URL for a team or portal site is specified, the crawl is restricted to the Document Library for that page. If you want to crawl the entire site, terminate the specified URL at the site path.

  Examples:

  http://sharepoint.example.net/sites/Mysite/SitePages/Home.aspx — Only the Document Library is crawled.

  http://sharepoint.example.net/sites/Mysite/ — The entire site is crawled, including the Document Library and any subsites.

- Links pointing to peer sites are not crawled. Specify the parent site or the site collection level in your scan, or create a separate scan for the peer site.

  Example:

  http://sharepoint.example.net/sites/Mysite/MySubSite/ is the URL specified in the scan. This subsite contains these links that you also want crawled:

  - *http://sharepoint.example.net/sites/Mysite/Shared%20Documents/Default.aspx*
  - *http://sharepoint.example.net/sites/Mysite2/Shared%20Documents/Default.aspx*

  To make sure these links and your subsite are crawled, specify this URL:

  http://sharepoint.example.net/sites/

- SharePoint links are case sensitive. When specifying the URL in your scan, verify that any capitalization matches exactly.
- When crawling a site that contains subsites, verify that the provided credentials have full read permission to access the subsites. Without the correct permissions, some subsites might not be crawled. For more information, see the Microsoft SharePoint documentation.
- Links pointing to pages outside the SharePoint site are not crawled.

Defining scans

Scans can be run to inventory and register documents, discover incidents, or classify data for an optimized scan.

The parameters that have to be defined depend on the scan type.

Classification scans are recommended before running Discover or Registration scans, because they provide information that allows you to focus on the most significant data types.

The scan definition must include the credentials to be used to access the repository. If the scan is not started manually, a scan schedule that determines when the scan will be run will also be needed.

Set up scans

Depending on your objective, you can set up scans that inventory, register, discover or classify data in file system or database repositories. Results from the classification scan type can be used to create optimized scans that produce better results faster.

Before you begin

Analyze your objective to determine the scan to run. You will need credentials for the file system or database repository.

Integrated Windows authentication is not supported for Microsoft SQL Server. If you are scanning a database server of this type, you must create an MS SQL Server user with the correct credentials.

McAfee recommends including the scan type in the name of a scan. For example, when you use the scan in the rule, a name like *Finance_registration* helps you remember what the scan does.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 In the **Actions** tab, select **New**.

3 Configure the **Node Definition** tab.

a Type in a scan task name and optional description.

b From the **Repository Type** menu, select a file system or database type.

The user interface offers different options for each type.

c From the **Credential** menu, select from the list of authentication parameters that allow access to the repository, or click **New** to add a new one to the list.

d From the **Schedule** menu, select from the list of default schedules, or click **New** to create a new one.

e From the **Mode** menu, select one of the four scan types.

f Under **Devices**, select the appliance from which the scan will be run. Select **None** if you want to save a scan without deploying it.

g In the **Node Definition** tab, define the server that is the target of your scan. Depending on the file system or database selected, you might enter a URL to define an FTP or web server instead of IP addresses or host names.

- For database scans, provide a port number, database login, and SSL certificate options along with an IP address or host name.
- For file system scans, provide one or more IP addresses, a subnet, or a range.

h To test the connection, select the device, then click **Test**.

i Click **Include** to add the defined node to the **Included** list.

To exclude one or more addresses from an IP address range or subnet, click **Exclude**.

4 Click the **Filters** tab to define the exact location on the server that you want to scan.

Depending on the repository type, you can filter by shares, folders, file properties on file system servers, or catalogs, schemas, tables, columns, and records and rows on database servers.

5 Click **Browse** to navigate to the location of the scan.

Alternatively, open the **Filter** category and set the options manually. If you choose this method, you can select **Preserve** to keep the original access times on the files. Otherwise, the operating system will change times tamps as the files are touched.

6 Click the **Advanced Options** tab to preserve the last access time, set the amount of bandwidth dedicated to the scan, and to configure email notifications to be sent when the scan starts or ends.

- If you choose to throttle the bandwidth available to the scan, enter a value in Kbps or Mbps.
- If you choose to send notifications of the start or end of a scanning process, you can use dynamic variables to provide scan details via email messages, but you cannot customize subject fields. There might be a lag of a few minutes between conclusion of the task and the posting of email notification, and file processing might continue after notification.

Setting **Last Access Time** to **Preserve** for an NFS scan on a model 4400, 5500, or virtual appliance is not supported.

7 Choose one of these options depending on the type of scan you are configuring.

- For an Inventory or Classification scan, configuration is complete.
- For a Registration or Data Match scan of a file system or database, click the **Registration** tab and select the **Signature Type** and **Target Devices**.
- For a Discover scan, click the **Policies** tab and select policies whose rules will be applied against data at rest in the defined repositories.

8 Click **Save**.

Filter scans by browsing

You can set the shares, folders and file properties to be scanned manually, or you can click **Browse** to set them by pointing and clicking.

Before you begin

Identify the file system or database that contains the target of the scan. Use the **Node Definition** tab to do this.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select **Actions** | **New**.

3 Type in a task name and select a **Repository Type**.

4 From the **Credential** menu, select **New**, enter the authentication parameters needed to access the repository, and save the credential.

5 From the **Schedule** menu, select **New**, set the scheduling parameters, and save the schedule.

6 Select the scan **Mode**.

7 Define the node to be scanned.

8 Click the **Filters** tab.

You must set the scan location manually if a URL is needed to access the repository.

9 Click **Browse**.

10 Select the repository from the directory tree in the repository.

Define scan locations manually

Define scan locations manually if parameters are easier to set one by one.

You can also browse to the location from the **Filters** tab.

Parameters in the **Advanced Options** and **Registration** tabs can be entered before or after the location is identified.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 In the **Actions** tab, select **New**.

3 Type in a scan task name and select a **Repository Type**.

4 If you have already created a credential, you can select it from the menu.

If not, you can create one while you are configuring the scan. Click **New**, enter the authentication parameters needed to access the repository, and click **Save**.

5 If you have already created a schedule, or you want to use one of the default schedules, you can select it from the menu.

Click **New**, set the scheduling parameters, and click **Save**.

6 Select the scan **Mode**.

You can inventory the scan target, register the data at that location, apply policies and rules, or classify the data.

7 Define the node to be scanned using an IP address, host name, or URL.

8 Click the **Filters** tab.

9 Expand the **Filter** menu.

10 Make selections from the menu categories to define the location of the scan.

11 Click **Save**.

Define an IP address or host name for a scan

Define scans by entering an IP address or host name of the file system or database repository to be crawled.

Before you begin

Define the scan operation name, credential, schedule, mode, and devices.

IP addresses or host names are required for most file system and database repositories to be scanned. If you are scanning a file system, you might define ranges of IP addresses or subnets to be scanned in one operation.

HTTP/HTTPS, FTP, and SharePoint servers require a URL instead.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 From the **Repository Type** menu, select a file or database server.

3 Type in the IP address or host name of the node to be scanned.

If you are scanning a **CIFS**, **NFS**, or **Documentum** file server, you can exclude IP addresses or ranges from the scan.

4 Click **Include** or **Exclude** to define the scan target.

5 Click **Test** to verify that the scan target is reachable.

6 Complete scan configuration by entering parameters in the **Filters**, **Advanced Options**, **Registration**, or **Policies** tabs as needed.

7 Click **Save**.

Define a subnet scan

Define a subnet scan by entering the base IP address as the first host IP of the sub-network. For example, you might use 172.25.6.1 as the base IP address, and 255.255.255.0 as the subnet mask.

You must use a valid address in the subnet range that can be considered the "starting" address to be scanned in the subnet. For example, if 172.25.6.14 is the IP address defined, 172.25.6.14 through 172.25.6.254 will be scanned.

You cannot use the broadcast IP address as the base IP.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 From the **Repository Type** menu, select a file or database server.

3 Type in the base IP address followed by the subnet mask (for example, 172.25.6.1/255.255.255.0).

4 Click **Include** to define the scan target.

5 Click **Test** to verify that the scan target is reachable.

6 Complete scan configuration by entering parameters in the **Filters**, **Advanced Options**, **Registration**, or **Policies** tabs as needed.

7 Click **Save**.

Define URLs to be scanned

Define URLs to define the target of HTTP, HTTPS, FTP, and Microsoft SharePoint repositories.

HTTP incremental crawls conserve bandwidth and other network resources. When HTTP servers are crawled the first time, every file is crawled and downloaded. In subsequent runs, only the files modified since the last run are downloaded. By dividing HTTP crawls into inventory and fetch phases that are run in parallel phases, only the fresh files, or those that have been modified, are downloaded.

Do not specify spaces in the URL. Use *%20* or + instead.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 From the **Repository Type** menu, select **HTTP**, **HTTPS**, **FTP** or **Microsoft SharePoint**.

Other repository types do not support URLs.

3 Select **Test** to verify that the URL is working.

4 Click **Include**.

5 Type in parameters in the **Filters**, **Advanced Options**, and **Registration** tabs as needed.

6 Click **Save**.

Define file properties to be used in a scan

Define file properties to be used in a scan of any of the supported file system repositories.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 After adding a scan operation and and defining the target in the **Node Definitions** tab, click the **Filters** tab.

3 Open the **Filter** category, then the **File Properties** menu.

If you are defining more than one file pattern, click **+** to add more elements.

4 From the **Condition** menu, select **equals** or **not equals**.

5 Type in a file property.

Examples:

- Absolute Directory Path > equals > C$/Eng/Network/Drawings
- File Pattern > equals > *.jpg
- File Owner > equals > bjones
- File Size > range > 1024–5000 (requires numbers expressed in bytes)

- File Creation Time > between > 16:30:00 and 17:00:00
- Last Modification Time > after > 13:30:00
- Last accessed > before > 17:00:00

6 Click **Save**.

Define shares to be scanned

You can define shares to be scanned only on CIFS, NFS, and Documentum repositories.

When you scan all shares, you do not have to define a filter. The default filter will always be set to crawl all the shares on the system from the root directory.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 After adding a new scan operation and defining the target in the **Node Definitions** tab, click the **Filters** tab, open the **Filter** category, then the **Shares** menu.

Equals is the only choice for finding shares; negative values cannot be used.

3 Select a condition.

The **All** condition is the default, indicating that all shares will be scanned.

Example: **Share** | **equals** `C$`.

If you select **Exact Match** or **Pattern**, enter a value that defines a specific directory or file pattern on the share.

4 Click **Save**.

Define folders to be scanned

You can define folders to be scanned only on CIFS, NFS and Documentum repositories.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Add a scan operation and define the target of the scan in the **Node Definitions** tab, then click the **Filters** tab.

3 Open the **Filters** category, then the **Folders** menu.

4 Type in the folders to be scanned on the share.

Absolute Directory Path is recognized as the base directory. All subdirectories matching the pattern will be crawled.

Examples:

- Absolute Directory Path > equals > C$/Eng/Network/Drawings
- Directory Pattern > contains > Human Resources
- Directory Pattern > does not contain > Employee Records

5 If more granularity is needed, define the file properties of the scan.

6 Click **Save**.

Define policies to be used in a scan

Define policies for a Discover scan to apply rules to data at rest in targeted repository. When a match is found, an incident is displayed on the dashboard and stored in the database.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 After adding a scan operation and defining the target in n the **Node Definition** tab, click the **Policies** tab.

3 Select one or more policies and **Add** or **Add All** to the **Selected Policies**.

Depending on the size of the repository, you will get better results from the scan if you select fewer policies.

4 Click **Save**.

Using credentials to authorize entry

Credentials are needed to authorize entry to repositories that are to be scanned.

Before you run a scan on a repository, you must have an account on it for which you can provide credentials. Some systems might also require a domain name to complete the authentication process.

If the data in a file system is openly accessible, you can use the default credential **None**.

Testing repository credentials

Repositories cannot be scanned without authentication. You can ensure that the repository is accessible by testing your credentials before you start the scan.

On the **Node Definition** page, you can click the **Test** button after defining the target of the scan. **Authentication failed**, **Success**, or **No Shares Detected** will appear.

If access to the repository is denied or the node definition is incorrect, the node will be highlighted in red; otherwise a green highlight will appear.

Add repository credentials

When you create a repository scan, you must already have a legitimate account on that repository. If you know what authentication parameters are required, you can use them to create a credential that will allow the scan to run.

Before you begin

Get the user name and password of an account on the repository that is to be scanned, or contact a system administrator to create an account for you.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Credentials**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Credentials**.

2 From the **Actions** menu, select **New**.

You can create a credential while you are configuring a scan by clicking the **New** button next to the **Credential** drop-down list.

The **Create Credential** window appears.

3 Type in a name and optional description.

4 Type in the user name of an account on the repository.

Domain name requirements vary by repository.

5 Type in the account password and confirm it.

6 Click **Save**.

Modify repository credentials

Modify credentials if the authentication parameters for the repository account have changed.

Before you begin

An existing credential must be displayed in the **Credentials** list.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Credentials**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Credentials**.

2 Click the **Name** of the credential to be modified.

The credential you create will be added to the drop-down list for use in subsequent scans.

The **Edit Credential** window appears.

3 Edit the **User Name** and **Password** fields.

Domain name requirements vary by repository. If the **Domain Name** has changed, you might also have to modify it.

4 Click **Save**.

Delete repository credentials

You can delete credentials that are no longer useful or valid. Only credentials that are not being used can be deleted from the system.

Before you begin

An existing credential must be displayed in the **Credentials** list.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Credentials**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Credentials**.

2 Select the credentials to be deleted.

3 Delete credentials in one of two ways.

- From the **Actions** menu, select **Delete Selected**.
- In the **Delete** column, click the trash can icon of the credential to be deleted.

Scheduling scans

Scans can be scheduled to run continuously, in periodic mode, or on demand. They can also be configured to run once, or not at all.

Daily, weekly, and monthly scan schedules are provided for easy application to new scan operations. They can be used on an as-is basis, or modified and customized. New scans can be added on the **Create Schedule** page in the **Classify** tab.

Add scan schedules

Add new scan schedules when needed by setting time parameters. Scans can be scheduled to run on a one-time basis, but they are often scheduled to run repetitively.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Schedules**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Schedules**.

2 From the **Actions** menu, select **New**.

3 Type in a name and optional description.

4 Set time parameters for the schedule.

Setting end times is optional.

5 Click **Save**.

Modify scan schedules

Modify scan schedules by editing parameters. Scans can be scheduled to run on a one-time basis, but they can also be configured to run repetitively.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Schedules**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Schedules**.

2 Click a schedule and modify the parameters.

3 Click **Save**.

Delete scan schedules

Delete scan schedules when you no longer need them. Only schedules that are not being used can be deleted from the system.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Schedules**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Schedules**.

2 Select the schedules to be deleted.

3 Delete schedules in one of two ways.

- From the **Actions** menu, select **Delete Selected**.
- In the **Delete** column, click the trash can icon of the schedule to be deleted.

Scan states

The status of each scan is displayed in the **Status** column on the **Scan Operations** page.

Table 14-20 Scan states

Scan status	Definition
Active	Task is ready to run and user can start tasks.
Running	Task (crawler) is running.
Inactive	Task has been removed from the schedule queue and tasks cannot be run (even manually). Such tasks must be activated before they can be run.
Starting	Task is starting and about to run.
Stopping	Task is stopping.
Stopped	Task was killed/crashed by some unforeseen situation. Such tasks can be started again. (Rare)
Aborting	Task is aborted immediately, discarding already fetched and queued objects, if any. This might lead to incorrect scan statistics (object counters) when the scan is next run.

Activate or deactivate scans

Scans must be in an active state before they can be run, and new scan operations are activated by default.

If you deactivate a scheduled scan, it will not run at the appointed time.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 From the **Actions** menu, select **Activate** or **Deactivate**

Start scans

Start scans on demand, or by scheduling them to start at a specific time.

Scans that are to be started must be in a **Ready** state.

A new scan will remain inactive until its associated policies are published.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scan to be started.

3 From the **Actions** menu, select **Start**.

Stop scans

Scans that are stopped shut down cleanly.

Before you begin

Scans that are to be stopped must be in a **Running** state.

Depending on the number of queued files and load on the server, it could be a few minutes to several hours before the processing of the crawled files is completed, and the task actually stops.

Stop does a clean shutdown of running tasks. When you stop a scan, the process pauses and the existing data is saved. All fetched files are processed, and all counters are updated before the scan exits and the system returns to readiness. Because of this, using **Stop** will not lead to missed files from processing.

Select **Start** from the **Actions** menu to resume the scan. Restarting the device is not necessary.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scan to be stopped.

3 From the **Actions** menu, select **Stop**.

Abort scans

Use the **Abort** function to stop scans quickly.

Before you begin

Scans that are to be aborted must be in a **Running** state.

Abort immediately kills a running scan without completing processing of files already fetched by the crawler. Some files might go missing due to the abrupt stop.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scan to be aborted.

3 From the **Actions** menu, select **Abort**.

Rescan a repository

Rescanning might be needed after a scan is stopped, aborted, when policies are changed, or file filters are updated.

When a repository is rescanned, the saved manifest is destroyed. Rescanning might result in duplicate incidents.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scan task you want to use to rescan the repository.

3 From the **Actions** menu, select **Rescan**.

Set bandwidth for a scan

By default, all available bandwidth is used when scanning. You can limit the amount of bandwidth used between McAfee DLP Discover and the scanned server.

Consider the transmission capacity of your network and the amount of network traffic before deciding how much bandwidth to allocate to the scan.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select a scan and click the **Advanced Options** tab.

3 Pull down the throttling menu and choose one of the following.

- **No Throttling** (default)
- **Kbps** (kilobits per second)
- **Mbps** (megabits per second)

4 Click **Save**.

On a 100-Mbps LAN, limit bandwidth to 50 Mbps to limit the crawler to half of the bandwidth available. If bandwidth is throttled correctly and there is L3 connectivity between networks, McAfee DLP Discover can be deployed across a WAN, though object viewing might be slower due to WAN latency. For example, if a 1 Gbps link between Tokyo and London is used, only ~10 Kbps throughput might be available for a CIFS scan.

Bandwidth throttling is applied as an average across the entire scan rather than as each individual file is being fetched. A Discover scan might burst above or below the configured throttle limit, but the average throughput measured across the entire scan will remain very close to the configured limit.

Managing scan load

Scan load might have an impact on performance of McAfee DLP systems. If too many operations are running concurrently, a scan might appear to be stalled.

Operations that add load to the system include:

- Deleting or creating scans in the same time frame
- Crawlers running and processing files from an extended scan
- Multiple policies and rules being decoupled from deleted scans
- Rescanning, which republishes associated policies and rules

If a scan appears to have stopped, wait for 30 minutes. If the task does not reactivate, select it and **Activate** from the **Actions** menu.

If several attempts fail, save the scan as a new task to republish all policies, and delete the old task.

Deploy scans

Scans that are deployed can be run from any of the defined appliances.

Signatures generated from managed McAfee DLP Discover devices are immediately loaded into **DocReg** when registration tasks conclude. They are automatically stored on other managed appliances to extend their usability.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scan to be deployed.

Scans are usually deployed when they are created, but not always. Deploying a scan to **None** saves it for later deployment.

3 On the **Edit Scan Operation** page, select one or more devices in the **Devices** box.

4 Click **Save**.

Modify scans

Modify scans if any of the defined parameters have changed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scan to be modified.

3 On the **Edit Scan Operation** pages, make changes to the scan parameters.

4 Click **Save**.

Delete scans

You can delete scans that are not producing the desired results.

Before you begin

A scan that is in a **Running** state must be stopped before it can be deleted.

When a scan is deleted, the incidents produced by that scan are saved. However, the original object that triggered the incident cannot be fetched or remediated from the incident dashboard, because the associated scan definition (credential/repository) metadata is lost.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scans to be deleted.

3 From the **Actions** menu, select **Delete**.

The scans immediately disappear from the list.

McAfee DLP Discover scan permissions

McAfee DLP Discover scan permissions must be set before users can scan repositories.

Table 14-21 McAfee DLP scan permissions

Scan permission	Definition
Manage Schedules	Create, edit, and delete schedules.
Manage Credentials	Create, view, edit, and delete credentials.
Manage Scans	Create, view, edit, activate, deactivate, and delete scans; register documents; view and export scan statistics, history, and registered files; add and view excluded text.
Control Scans	Create new actions, view, start, stop, re-scan, and clone tasks; view and export scan statistics, history, and registered files; add and view excluded text.

Set scan permissions

You must assign scan permissions privileges to users who will be using McAfee DLP Discover to scan repositories.

Before you begin

You must have administrator permission to perform this task.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Click **Details** for the user group.

3 Click **Task Permissions**.

4 Open **Discover Scan Permissions**.

5 Select one or more permissions.

6 Click **Apply**.

McAfee DLP Discover registration permissions

McAfee DLP Discover registration permissions must be set before users can register data.

Table 14-22 Registration permissions

Registration permission	Definition
Web Upload	Upload documents or structured data to be registered; no deletion or de-registration rights; view user's own registered documents.
Manage Uploaded Documents	Upload documents or structured data to be registered; view and manage documents uploaded by all users; delete and deregister uploaded files; update and delete excluded text.
Discover Registration	Register documents or structured data.

Set registration permissions

Set registration permissions to assign privileges to users who will be using McAfee DLP Discover to register data.

Before you begin

You must have administrator permission to perform this task.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Click **Details** for the user group.

3 Click **Task Permissions**.

4 Open **Discover Registration Permissions**.

5 Select one or more permissions.

6 Click **Apply**.

Users might also need **Incident Permissions**.

Managing discovered files

McAfee DLP Discover protects data by finding and displaying sensitive data. Remedial actions can be pre-programmed to resolve any problems found.

When a violation is found, you can use a **Data-at-Rest** action rule to prevent or resolve the problem.

Use the **Remediation** button on the **Incident Details** page to resolve incidents as their components are reviewed.

Remediation is part of the incident workflow, and any time incidents are wiped from the system, remediated files will also be wiped.

When violations are found in **Data-at-Rest**, the remediation feature might be used to do the following:

- Copy files containing violations to another location on the network
- Move files containing violations to another location on the network
- Encrypt files containing violations
- Delete files containing violations

Each of these actions also includes the capability to do the following:

- Notify users of violations found in scanned data
- Record violations found in scanned data in a system log
- Assign incidents to one or more reviewers
- Set a status that indicates the state of resolution

Remediation can be applied directly to incidents reported on the **Data-at-Rest** dashboard, or pre-programmed by attaching an action rule to rules that produce incidents.

Types of remedial actions

Remedial actions can be set up to copy, move, encrypt and delete incidents found in **Data-at-Rest**.

Incidents found by a Discover scan might be processed using one of four remedial actions.

- Copy the file to another location
- Move the file to another location
- Encrypt the file
- Delete the file

You can configure the copy, move, and encrypt actions to automatically notify users that a remedial action has been applied.

You can configure any action to place a record in a system log, assign the incident to one or more reviewers, or apply a status that indicates its stage of resolution.

Compliance with FIPS standards

With this release, best practices for implementing cryptographic algorithms, which handle key material and data buffers, are supported by compliance with FIPS standards.

The Federal Information Processing Standard (FIPS 140-1) and its successor (FIPS 140-2) are U.S. government standards that provide a benchmark for implementing cryptographic software. Algorithms used for encryption, hashing, and signing are enabled to secure the McAfee DLP Discover remediation processes.

Review remedial actions

You can review remedial actions that have been applied to an incident on the **Incident Details** page.

Click **Columns** to add the **RemActionType** and **RemTaskStatus** columns to the dashboard.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select **Data-at-Rest** from the display thumbwheel.

3 Click **Details** for an incident.

The **Incident Details** page appears.

4 Review the remedial actions that have been applied.

Add columns to display remedial actions

Add columns to configure the **Data-at-Rest** dashboard to display remedial actions that have been applied to incidents.

If you make a mistake, you can move column headers out of the **Selected** list by selecting them and clicking **Remove**.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select **Data-at-Rest** from the display thumbwheel.

3 Click **Columns**, then scroll down the list of **Available** columns.

4 Select one or more of the **Remediation** column headers:

- **RemActionType**
- **RemTaskStatus**

5 Click **Add** to move the column headers to the **Selected** list.

6 Click the **Move Up** and **Move Down** buttons to position the columns on your dashboard.

Moving column headers to the top of the window positions them on the right side of the dashboard.

7 Click **Apply**.

The **Incidents** dashboard displays the added columns.

Add remedial action rules

Add remedial action rules to rules that will be used in a Discover scan. When the rule hits, the action will be applied.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu under **Data-at-Rest**, select **Add Action Rule**.

3 Type in a name for the action rule.

4 Open **Email Notification** to alert one or more users to the action.

5 Open **Syslog Notification** and select **Enable** to log the incident.

6 Open **Incident Reviewer** and select **Incident Status** to assign a reviewer.

7 Open **Incident Status** to define its stage of resolution and select **Enable** to log the incident.

8 Open **Remediation Policy** and select the corrective action that is to be taken.

9 Click **Save**.

Apply remedial action rules

Apply remedial actions to discovered incidents by adding them to rules. The actions are applied when the rule is matched against on data at risk. If the rule detects sensitive data, the action defined in the rule will be taken.

If McAfee DLP Discover and McAfee DLP Monitor devices are managed by McAfee DLP Manager, every rule can be configured to deploy one action to each of the three incident types.

Rescan to produce updated results, then verify that the action rule applied to the rule implements the correct remedial action.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click the policy defined in the scan, then click a rule.

3 Click the **Actions** tab.

4 Click **Add Action**.

5 Select a remedial action from the **Data-at-Rest** menu.

6 Click **Save**.

Set up locations for exported files

Set up locations for exported files so that when sensitive files are found in a database or repository, they can be copied or moved to a shared folder.

Export locations are used in file remediation and action rules.

Only Windows shares (CIFS) are supported.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Export Locations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Export Locations**.

2 From the **Actions** menu, select **New**.

3 Type a location on the **Create Export Location** page.

If the folder does not already exist, it is created.

4 Select a credential to access the repository, or click **New** to create a new using the authentication parameters of an existing account.

5 Click **Test** to verify read/write access to the repository. If the credential is correct but the test is negative, use Windows Explorer to verify that sharing is enabled and read/write privilege has been granted.

6 In Microsoft Windows Explorer, right-click the target folder and select **Properties**.

7 In the **General** tab, deselect the **Read-only** checkbox.

8 In the **Sharing** tab, select **Share this folder.**

9 Click **OK**

10 Click **Save**, then re-test.

Copy discovered files

Copy discovered files to a quarantined export location after a remedial action has been applied to an incident.

When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

You can use **Dynamic Variables** to automatically inform users that the file has been copied to an export location.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule**.

- If you want to copy an incident from the dashboard, click **Details**, select **Remediate** | **Action**, then select the **Copy** action rule from the sub-menu.
- If you want an incident to trigger a copy action, add the <copy action rule> to the rule and click **Save**, then start a Discover scan that applies the rule containing the action rule.

3 Type in a name for the action rule.

4 Open **Email Notification** to alert one or more users when the action is triggered.

You can use **Dynamic Variables** to inform users of the prevented action automatically.

For example, `##Filename` found by the `##Rule` violated the `##Policy` and was copied to <export location>.

For example, `##Filename` found by `##ScanOperation` violated the `##Policy` and was copied to <export location>.

5 (Optional) Open **Syslog Notification** and select **Enable** to log the incident.

6 Open **Incident Reviewer** to assign a reviewer when the action takes place (recommended).

7 Open **Incident Status** to change the stage of resolution when the action takes place (recommended).

8 Open **Remediation Policy** and select **Copy** from the **Action** list.

9 Select the export location from the **Destination** drop-down list.

10 Click **Save**.

Move discovered files

Move discovered files to a quarantined location after a remedial action has been applied to an incident.

When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

You can use **Dynamic Variables** to automatically inform users that the file has been moved to a quarantined location.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule**.

- If you relocate an incident from the dashboard, click **Details** and select **Remediate** | **Action**, then select the **Move** action rule from the sub-menu.
- If you want an incident to trigger a move, add <move action rule> to the rule and click **Save**, then start a Discover scan that applies the rule containing the action rule.

3 Type in a name for the action rule.

4 Open **Email Notification** to alert one or more users when the action is triggered.

You can use **Dynamic Variables** to inform users of the prevented action automatically.

For example, `##Filename` found by the `##Rule` violated the `##Policy` and was quarantined.

For example, `##Filename` found by `##ScanOperation` violated the `##Policy` and was moved to <export location>.

5 Open **Syslog Notification** and select **Enable** to log the incident (optional).

6 Open **Incident Reviewer** to assign a reviewer when the action takes place (recommended).

7 Open **Incident Status** to change the stage of resolution when the action takes place (recommended).

8 Open **Remediation Policy** and select **Move** from the **Action** list.

9 Select the quarantine location from the **Destination** drop-down list.

10 Click **Save**.

Encrypt discovered files

Encrypt discovered files when they are found by providing passwords that must be used to access them. With this release, the default *openssl* utility used to encrypt discovered files is replaced with the McAfee® Endpoint Encryption for Files and Folders algorithm.

The encryption key is stored in ePolicy Orchestrator databases and an ePolicy Orchestrator extension is used to display the list of keys stored.

When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

You can use **Dynamic Variables** to automatically inform users that the file has been encrypted.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule**.

3 Type in a name for the action rule.

4 Open **Syslog Notification** and select **Enable** to log the incident (optional).

You can use **Dynamic Variables** to inform users of the encryption automatically.

For example, `##Filename` found by the `##Rule` found by the `##ScanOperation` was encrypted.

5 Add **File Marker Text** to change the stage of resolution when the action takes place (recommended).

6 Open **Incident Reviewer** to assign a reviewer when encryption occurs (recommended).

7 Open **Incident Status** to change the stage of resolution when encryption occurs (recommended).

8 Open **Remediation Policy** and select **Encrypt** from the **Action** list.

9 Enter a password and confirm it.

10 Click **Save**.

Delete discovered files

Delete discovered files by a delete action when they are found by a Discover scan. After this is done, the file cannot be recovered.

When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

You can use **Dynamic Variables** to automatically inform users that the file has been deleted.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Action Rules**.
- On your McAfee DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule.**

- If you relocate an incident from the **Incident Details** page, select its checkbox and select **Remediate** | **Action** and select the **Move** action rule from the sub-menu.
- If you want an incident to trigger a move, add the <delete action rule> to a rule and click **Save**, then start a discovery scan that applies the rule containing the action rule.

3 Type in a name for the action rule.

4 Open **Remediation Policy** as appropriate.

You can use **Dynamic Variables** to inform users of the prevented action automatically.

For example, `##Filename` found by the `##Rule` found by the `##ScanOperation` was deleted.

5 Add **File Marker Text** to change the stage of resolution when the action takes place (recommended).

6 Click **Save**.

7 Apply the new action rule to one or more rules.

8 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations**.

9 When the **Scan Operations** page appears, select a scan.

10 From the **Actions** menu, select **Rescan**.

11 Check the results to verify that the file has been deleted.

Revert remediated files

Revert remediated files to reverse an action that has been applied to a file that was found during a scan.

Deleted incidents cannot be reverted or recovered.

If data is moved to quarantine an incident, the action can be reverted. If remediation actions fail, error messages appear.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select one or more incident checkboxes.

3 From the **Remediate** menu, select **Revert**.

4 Click **OK** to confirm, or **Cancel**.

5 You might want to rescan to verify that the action has been reverted.

Scan statistics and reports

When you run a scan operation, files that have been registered or matched to rule conditions are indexed and fetched from the repository. Incidents found by the crawler are displayed under the **Data-at-Rest** vector.

Scan results are first displayed on the **Scan Statistics** dashboard. Statistics describing the status of the scan are displayed under **Statistics** on the **Scan Operations** page.

Incidents found by a scan operation are reported on the **Data-at-Rest** dashboard. Files are downloaded directly to McAfee DLP Discover from the host on which they were detected, but the files are not saved indefinitely. They are fetched from the source when needed and the cache is flushed regularly to optimize disk utilization and keep copies of sensitive information from being stored on the system.

The index keeps running in the background until all files are reported, even if the task has completed.

To maximize performance during CIFS, NFS, or Documentum inventory scans, the crawler updates the database only after 100,000 files have been processed. If fewer files are detected, the counters are updated after the scan has been completed.

Scan results are reported on the **Data-in-Use** dashboard, but the scan metadata is available on the **Scan Operations Statistics** page.

Statistics include the parameters defined in the scan and processing information about the crawl, such as files processing, number of incidents retrieved, and success of the run.

When you run a scan operation, files that have been registered or matched to rule conditions are indexed and fetched from the repository. While files are being fetched, counters increment as nodes are identified and shares are authenticated. The incident database is updated every 15 minutes until the conclusion of the task.

View scan results

When you run a scan, files that have been registered or matched to rule conditions are indexed and fetched from the repository, and any incidents detected are displayed on the **Incidents** dashboard under the **Data-at-Rest** vector.

You can find the results of in-progress or completed scans on the **Scan Statistics** page. View specific matches for each incident by clicking its **Details** icon.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Select the scan and click **Statistics**.

3 View the details in the **Job Summary** tab.

4 Click the **Repository Detail** tab for more information.

The **Host Summary** and **Share Details per Host** drop-down menus appear.

5 Open the menus and click the underlined values for more information.

If useful information is reported, select **Export** to save it to a CSV file.

Determining access to scanned files

When incidents are reported, the **Access Control List** for each file can be viewed in incident details. During scans, file metadata and permissions are fetched first, and permissions are reported on the **Incident Details** page.

View the list of scanned files

View information about files discovered in a scan, such as the file name, path, file size, and last modified date.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 In the **Objects** column, click the displayed number for the scan.

The **File List** page appears.

File sizes without a unit are listed in bytes.

Export reports of scan statistics

The results on the **Scan Operation Statistics** page can be exported to reports.

All results generated during a scan are saved and appear on dashboards.
If you have Microsoft Excel installed and are using Internet Explorer, the reports automatically open in Excel. If not, a comma-separated values (CSV) text file opens.

Because CSV is a generic ASCII format, it can be opened with any text editor, spreadsheet, or database program. If the CSV file is very large (50,000 or more records), it will be compressed into a .zip file before it is available for opening or saving.

Generated reports are kept for 30 days from the last access date. Reports that have not been accessed in 30 days are removed to free up disk space. Generated reports are removed when the system is upgraded or restored from a configuration backup.

Exported reports are shared across all users.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Click **Statistics**.

3 From the **Report Options** menu, select **Export File List**. The **Discover Window Reports** window appears.

4 [Optional] Add an email address to notify when the report completes.

a In the **Email To** field, enter an email address.

b Click **Update**.

Leave the **Email To** blank if you do not want to be notified.

5 To check the status of reports, click **Refresh**.

6 Click **Download** when the export completes.

Types of scan statistics reports

Three types of scan statistics reports can be generated.

Table 14-23 Types of scan statistics reports

Report type	Description
Current statistics	Reports statistics which are currently viewable. They could be from the current scan, the last one run, or any other historical scan.
All statistics	Reports all the statistics of all the runs of the scan task
Export file list	Reports the file list at share level (only files of the required share), IP level (only files of a required host), or task level (all files detected by the task across hosts and shares). If there is a single host with a single share, all three reports will be the same.

Get historical scan statistics

You can get historical statistics from previously completed scans by selecting an export option from the **Report Options** menu in McAfee DLP Discover.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations** | **Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations** | **Scan Operations**.

2 Click **Statistics**.

3 From the **History** menu, select a scan.

Types of task status messages

McAfee DLP Discover task status messages advise users of scan anomalies.

Table 14-24 Types of task status message

Status message	Definition	Remedy
Resource Missing	The path does not exist, or the file might be missing. It was found during the investigation phase (indexing), but is missing during the crawling phase.	Check on the repository to see if it is really missing. If not, restart the scan.
Configuration Error	The task database might have been corrupted.	Recreate the task. Call McAfee Technical Support if that does not resolve the problem.
Connection timed out - Incomplete Listing	Cannot connect to the repository while investigation phase is in progress.	Wait for awhile, then try again.
Complete	The scan is complete.	
Incomplete	The scan is incomplete, probably due to a network error. The repository might have become unavailable.	Reconnect and restart the scan.
Incomplete Listing	The node is down, there was a network failure, credentials were changed between tasks, or the server is busy.	Wait for awhile, then rescan.
Server stopped responding	The server is busy.	Wait for awhile, then resume the task.
Task Terminated	The Stop action was applied to the scan operation, the task stopped according to schedule, or it was killed by some extraneous means (for example, a system crash or health check).	Wait for awhile, then rescan.
Task Terminated - Incomplete Listing	The task stopped (or its scheduled end time arrived) during investigation phase.	Restart the task.
Waiting - crawlers busy	The system has reached the maximum limit.	The task will continue when the system is free.

Types of system status messages

McAfee DLP Discover system status messages advise users of scan anomalies.

Table 14-25 Types of system status message

Status message	Definition	Remedy
Connection Timed Out	The repository is busy, too many connections have been made to the repository, or the network is down.	Make sure the repository node is accessible from the McAfee DLP Discover appliances network, wait for the network or repository to idle, then restart the scan.
Account is locked	The account (username) is locked.	Provide a valid account, or contact administrator of the repository.
Authentication Failed	An incorrect credential has been entered.	Check the user name, password, and domain in the credential, or try another one. This error might appear when using domain credentials or if the domain controller (for example, Active Directory) is down.
Authentication OK	Authentication was successful.	

Table 14-25 Types of system status message *(continued)*

Status message	Definition	Remedy
Permission Denied	Although authentication was successful, you do not have the permission needed to use the resource.	Contact your administrator.
Do not have permission to update last access time on repository	Permission is needed to access the repository.	Supply the correct credentials (read/write access) and restart the task.
Share (or Shares) Inaccessible	A share might be inaccessible because of insufficient user privilege, or because the share is being used exclusively by another process.	Select the **Filters** tab and try to browse to the share.
Socket Communication Failure	Could not establish a socket connection to the database.	Verify the IP address and port, then restart.
Unknown	This error is rare but might be related to a configuration error.	Call McAfee technical support if the error persists.
Unknown database	The login database given was wrong.	Provide the correct login database, then restart.
Unsupported database version	Database version on the repository is not supported.	Check the documentation for the supported version.

Typical scenarios

Use these scenarios to understand ways to use McAfee DLP Discover to perform routine scanning tasks.

Scheduling lengthy scans to run at regular intervals

When you schedule a scan to run at regular intervals, it will run until it completes unless an end time is defined on the **Schedule** page. If the scan is still running at the time of the next scheduled interval, that instance is skipped, and scanning restarts at the following one.

For example, if a daily scan that has no end time starts running on Monday at 9 a.m. and completes 49 hours later, it will restart Thursday at 9 a.m.

Create a one-time scan that runs until it completes

When you schedule a scan with a start time but no end time, it will run until it completes.

Before you begin

Determine the repository type, the credentials used to access it, and the scan mode that fits the task. For example, if you are scanning a Windows repository to find HIPAA violations, you will want to create a CIFS Discover scan.

Alternatively, you could run the complete scan at the desired time by selecting **Start** from the **Actions** menu on the **Scan Operations** page. It will run to completion as long as you do not select **Abort** or **Stop** after the scan starts running.

This scan requires completion of three different user interface elements: **Scan Operations**, **Schedules**, and **Credentials**.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations**.
   - On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations**.

2 From the **Actions** menu, select **New**.

3 On the **Add Scan Operation** page, type a name and optional description.

4 In the **Devices** frame, select the Discover device from which the scan will run.

   If you are not planning to run the scan right away, click **None**.

5 From the **Repository Type** menu, select **CIFS**.

6 Click **New** to add a credential, or accept the **none** default.

   The **Create Credential** window appears. Type in the user account information you need to access the repository, then click **Save**.

7 Click **New** to add a schedule, or accept the **none** default.

   The **Create Schedule** window appears. Enter a name and optional description, select **Once** and **No End Time**, set a **Start Time** for the scan, then click **Save**.

8 From the **Mode** menu, select **Discover**.

9 In the **IP Address/Host Name** field, type the IP address or host name, then click **Test**.
   - If the host is not found, check the credentials and determine if the system is up.
   - If the test is successful, click **Include**. The credential will be checked in the background, and the IP Address or Host name will be highlighted in a color that indicates the success or failure of the automatic testing.
     - Green highlighting indicates a successful connection.
     - Red highlighting indicates a failed connection.
     - Amber highlighting indicates partial success. This might occur if multiple hosts or IP ranges are included, because only a small subset of nodes are tested.

10 In the **Filters** tab, click **Browse** to locate the share to be scanned, or set the **Filter** category options to define it.

11 In the **Advanced Options** tab, set the bandwidth to be used for the scan, or accept the **No Throttling** default.

12 If you want to retain the timestamps on the files after scanning, select **Preserve Last Access Time**.

13 If you want to send notification of start or end times, type in the associated email addresses.

   Set the dynamic variables in the **Message** fields if you want to provide specific information about the scan.

14 In the **Policies** tab, select at least one policy to define the rules that are to be applied against the data at rest in the repository, then click **Add**.

15 Click **Save**.

The **Scan Operations** page appears.

16 Select the scan to be run.

17 From the **Actions** menu, select **Start**.

The **Status** column will change to indicate that the scan is **Initializing**, then **Running**.

18 Click **Statistics** to check the progress of the scan.

Create a scan that runs only when started manually

When you create a scan, a **Schedule** parameter must be included. But the default setting is **none**, and if you accept it, you must run the scan manually.

Task

1 Create and save a scan operation with **Schedule none** and a **Device** selected.

In the **Advance Notification** tab, provide email addresses so you will know when the scan starts and stops.

2 On the **Scan Operations** page, select the scan and select **Activate** from the **Actions** menu.

Only scans that have been deployed on a McAfee DLP Discover appliance can be activated.

The **Status** column changes from **Inactive** to **Ready**.

3 From the **Actions** menu, select **Start**.

The **Status** column changes from **Ready** to **Initializing**, then **Running**.

4 Click **Statistics** to monitor the progress of the scan.

When the scan completes, the **Status** column changes from **Running** to **Ready**.

Identify and track sensitive documents

When you upload a document to McAfee DLP Discover, a series of overlapping tiles are given hexadecimal numbers that stamp each segment with a unique identity. Even if words are transposed, or contents differ by a few lines of text, each component of the document can be tracked.

If you can't upload all of your sensitive data because you can't identify it all, run a Discover scan that applies a generic set of rules against the data in your repository. You can set it up so that it will generate incidents that violate many different policies, and when you evaluate the results you can devise a more targeted strategy.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Registered Documents**.
- On your McAfee DLP appliance, select **Policies** | **Registered Documents**.

2 From the **Actions** menu, select **Upload New File**.

3 Browse to locate a sensitive file that must be protected.

Mozilla Firefox 3.5 will not include the path to the uploaded document unless you reconfigure it before scanning.

4 Select a policy and rule to guide the search.

For example, select the *Financial and Security Compliance* policy and the *Financial Statement Documents* rule to protect a document that contains sensitive financial information.

5 If more documents need protection, select **Save & Upload Another** and repeat the process.

6 Click **Save**.

7 After some time, check the **Data-at-Rest** vector on your McAfee DLP Manager dashboard. For full coverage, add the content to a rule and schedule it to run at regular intervals.

Remember to select an appropriate time filter. The system cannot track data before it was uploaded.

Control copies of sensitive documents

Confidential documents often proliferate over networks, because employees can copy or move them to insecure locations to work on them, or share them with other staff members. You can find sensitive documents that have been copied or moved by using their signatures.

Task

1 Create a Discover scan to find the file on the targeted repository.

The scan will produce a list of incidents on the **Data-at-Rest** dashboard.

2 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

3 Select **Data-at-Rest** from the vector thumbwheel and click **Columns**.

4 Add the **Signature** and **Path** columns to your dashboard, then click **Apply**.

5 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Registered Documents**.
- On your McAfee DLP appliance, select **Policies** | **Registered Documents**.

6 On the **Web Upload** page, click **View** to locate the signature number, and copy it.

7 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

8 Open the **File Information** category and select **Signature** | **is any of** , then paste the signature number in the value field.

9 Click **Search**.

All incidents containing the file with that unique signature will be reported to the dashboard.

10 View the **Signature** and **Path** columns, which will tell you the exact locations of the file.

15 Incident dashboards and reports

Incidents reported by the McAfee DLP products are captured, detected, or generated by the McAfee DLP products and stored in three different databases.

Table 15-1 McAfee DLP dashboards

Dashboard	Definition
Data-in-Motion	Incidents are produced by McAfee DLP Monitor and McAfee DLP Prevent when its rules match data in the network stream.
Data-at-Rest	Incidents are produced by McAfee DLP Discover when a scan finds sensitive data in network repositories or databases.
Data-in-Use	Events are produced by McAfee DLP Endpoint when data violations are found at network endpoints, and they are copied over from McAfee ePolicy Orchestrator to McAfee DLP Manager.

Contents

- *Using the Home page*
- *Managing incidents*
- *Customizing dashboards*
- *Troubleshooting dashboard incidents*
- *Generating reports*
- *Typical scenarios*

Using the Home page

The **Home** page is used to provide summaries of the problems found by McAfee DLP appliances.

The **Home** page contains a configurable selection of dashboards that contain information about your network and endpoint data. An administrator might set a default configuration depending on the needs of a user group, and users can customize your own view by selecting from the wide variety of dashboard configurations available on the **Options** page.

The **Data-in-Motion**, **Data-at-Rest**, and **Data-in-Use** dashboards display incidents and events that have been generated by the McAfee DLP products, which protect data found in network traffic, repositories, and at network endpoints.

The **Home** page contains report summaries. The **Incidents** dashboard must be used to sort, filter, or manage the incidents.

The **Home** page is configurable to provide information about the monitored systems at a glance. Each user can set up to four dashboards that appear immediately after logon.

Customize the Home page

Customize the **Home** page to display reports of the most significant incidents and events found by the McAfee DLP appliances. Four different dashboards can be displayed on the same landing page.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **DLP Homepage**.
   - On your McAfee DLP appliance, select **Home**.

2 Click **Options** and select **Customize**.

3 On the **Dashboard Type** page, select the checkboxes of one of the four dashboards.

4 To configure the display of Dashboard 1, select one of two options:
   - Select **Pre-defined** and select one of the pre-configured dashboards from the drop-down list.
   - Select **Chart**, name the dashboard, then select from the options available.

5 Repeat the process for Dashboards 2, 3, and 4.

6 Click **Apply**.

Assign Home page permissions

If you are an Administrator, you can assign task permissions to users who will be using the **Home** page.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups**.
   - On your McAfee DLP appliance, select **System** | **User Administration** | **Groups**.

2 Click **Details** next to the user's group.

   The **Group Name** page appears.

3 Click **Task Permissions** and open the **Incident Permissions** category.

4 Select the **View Home page** checkbox.

   Users who do not have this permission will not be able to see the **Home** page.

5 Click **Apply**.

Managing incidents

Use the incident dashboards to view, sort, and manage your incidents.

Sort incidents

The capture engine sorts all network data and stores it in the McAfee DLP databases. Each object in the database is defined by its attributes, which can be used as a key to rearrange the data to reveal significant patterns.

Each column on the dashboard displays a different attribute of the object in the database. The objects can be sorted by attribute by clicking in the table header.

Attachments to incidents can be displayed if they are under 50 MB, and the number of incidents that can be reported is limited to 150,000 per data loss vector. After that number is reached, chunks of supporting data are wiped, starting with the oldest incidents first.

Sorting allows you to set aside results that are not immediately relevant, but might be significant at a later date. Save a view or report to revisit the data.

Sort incidents by attribute

You can sort incidents that have attributes in common by clicking on a column header.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click a column header to sort by attribute.

The dashboard displays all incidents that have that attribute in common.

Sort incidents by policy

Find policy violations by selecting the incidents in the display pane, then viewing the policy and rule names displayed in the navigation pane.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select one of the policies listed in the **Group by** frame. The incident listing displays only incidents found by that policy.

Violations are grouped by policy by default.

Delete incidents

Delete incidents that are not useful to clear the display pane for significant results.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select the checkboxes of incidents to be deleted.

3 From the **Actions** menu, select **Delete**.

Delete similar incidents

Delete similar incidents if they are no longer useful, or if they share attributes that trigger false positives.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click on a column header that identifies the attribute shared by the false positive incidents.

3 Select the checkboxes of incidents that share the attribute.

4 From the **Actions** menu, select **Delete**.

Filter incidents

The capture engine sorts captured data into objects and their attributes, which are displayed in the rows and columns on the dashboards.

Each incident displayed on the McAfee DLP dashboard is supported by a wide range of supporting data. So many incidents are reported that grouping and filtering is necessary to display only those that are significant.

Filters can be added to the incident dashboard whether or not there are values in an attribute field. Click on any data cell, even if it is empty, to use the attributes of an incident as a sorting key.

Set a time filter for incidents

Set a time filter to limit the incidents displayed to a relative time frame. Customized dates can also be set to define a specific time frame.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click the **List** button, if necessary.

List is the default dashboard view.

3 From the **Filter by** menu, select a time frame. If you select **Custom Dates**, click **?** to launch input fields.

The time frame must not exceed the limits of the data captured. Outside of those specific limits, incidents cannot be found. For example, if you select **Yesterday** but your McAfee DLP appliances were set up **Today**, you will filter out everything on your dashboard.

4 Click **Apply**.

Filter incidents

Filter incidents that have been reported to the dashboard into configurations that reveal significant data patterns.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click the **List** button, if necessary.

List is the default dashboard view.

3 In the **Filter by** pane, pull down the second timestamp menu to select a time frame. If you select **Custom Dates**, click the **?** to launch input fields.

The time frame must not exceed the limits of the data captured. For example, if you select **Yesterday** but your McAfee DLP appliances were set up **Today**, you will filter out everything on your dashboard.

4 Click **+** to add another sorting key.

5 Click **Apply**.

6 Repeat as needed until a significant data pattern is revealed.

Group incidents

Group incidents that have been reported to the dashboard into configurations that reveal significant data patterns.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click **Group Detail**.

3 From the **Group by** menu, select a primary sorting key for the incidents on the dashboard.

4 From the **Group by** menu, select a secondary sorting key for the incidents on the dashboard.

5 Change the groups as needed until a significant data pattern is revealed.

Clear filters

Clear filters to release configurations that display a specific set of attributes. When incidents are filtered, the configuration will block all other results until the filter is cleared.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.
2 Click the **List** button. It is the default dashboard view, so the display might not change.
3 In the **Filter by** pane, click **Clear All**.
4 Click **Apply**.

Getting incident details

The **Incident Details** page provides in-depth information about each incident or event detected by the McAfee DLP system.

View incidents

View contents of incident by clicking **Details** for each incident reported to the dashboard. The **Incident Details** page displays the elements that make up each incident.

Incidents that are captured in real time, like chat and FTP sessions, cannot display details (like file names and user information) because they cannot be synchronized with the existing flow.

If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.
2 Select an incident and click **Details**.
3 Select from the tabs and links on the page.

   Clicking an attachment (**Info** | **Content**) will launch the file if the corresponding software is installed.

Get case status

Find the case status of incidents by clicking **Details**. The **Incident Details** page displays the case status for incidents.

If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.

2 Select an incident and click **Details**.

3 Click **Cases**.

View related incidents

When an incident is viewed on the **Incident Details** page, **Related Incidents** might also be displayed.

Before you begin

Related incidents are based on values in six fields: Signature, File name, Source IP, Destination IP, Sender, and User ID.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select an incident and click **Details**.

3 View the statistics in the **Related Incidents** tab in the right pane.

Find the concept that matched

Find the concept that triggered the incident by clicking **Details** to launch the **Incident Details** page. The page displays the concept used as well as the match strings defined in the concept.

If you cannot see incident details, you need **View Incident Object** permission. See your administrator.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select an incident and click **Details**.

The **Incident Details** page appears.

3 View the **Concepts** section in the **Related Incidents** tab.

Find match strings

Find the match string that triggered the incident by clicking **Details** to launch the **Incident Details** page. The page displays the alphanumeric strings defined in the concept, rule or query.

If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select an incident and click **Details**.

The **Incident Details** page appears.

3 You can find the alphanumeric string in the **Match String** tab.

Set incident states

Incidents might share some of the same states. If not, they can be assigned directly from the dashboard by clicking the **Attributes** button. You can set them from the **Incident Details** or **Incident List** pages.

States are referred to as *attributes* in the user interface, but that term generally refers to the characteristics that define a database object. The states available for modification are **Status**, **Reviewer**, **Resolution**, **Severity**, and **Comments**.

If you do not have permission to view a state, it will not be displayed for modification.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select one or more incidents whose attributes you want to modify.

3 Do one of the following:

- If you want to modify states from the incident listing, click **Attributes** in the dashboard header. Select the checkboxes of the attributes to be modified, then select a new value from the drop-down menu and click **Apply**.
- If you want to modify states from the **Incident Details** page, click **Details**. Select new values from the drop-down menus, and add optional comments.

Get incident history

Get the history of an incident by clicking **Details**. The **Incident Details** page displays the actions have been taken in the **History** tab.

If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select an incident and click **Details**.

3 Click the **History** tab.

Set up incident views

Pre-configured dashboard views reflect the content of the incident and event databases. They can be selected from the **Incident Listing** menu, and custom views are automatically added to the list.

When incidents are grouped and filtered, significant data patterns emerge. When this happens, the configuration can be saved so that it can be re-used as new incidents are added over time.

Attachments to incidents can be displayed if they are under 50 MB, and the number of incidents that can be reported is limited to 150,000. After that number is reached, chunks of supporting data are wiped, starting with the oldest incidents first.

Select different views from the **Incident Listing** menu to get ideas about how to filter your results.

Save home views

Save home views to keep the incident configurations you find most useful. Saving effective configurations allows re-use when new incidents are found.

To save the content of a dashboard view instead of the settings, create a report.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **My Views**.
- On your McAfee DLP appliance, select **Incidents** | **My Views**.

2 Click a view.

3 On the **View Properties** page, name the view.

4 Set an owner.

Ownership is determined by the groups to which a user belongs. If the group needed is not listed, add a new one and assign a user to it.

5 If you want this to be your landing page, select the **Set as Home View** checkbox.

6 Click **Save**.

Select pre-configured views

Pre-installed views display incidents in a wide variety of configurations.

This is a good way to figure out how to filter your incidents into the most significant data patterns.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select any view from the **Incident Listing** menu and review the results.

Select view vectors

Select view vectors to display incidents from three different databases.

Table 15-2 View vectors

Vector	Database
Data-at-Rest	Static data found in network file systems or databases
Data-in-Motion	Dynamic data found in network traffic
Data-in-Use	Static data found at network endpoints (computers, removable media, printers, etc.)

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select **Data-at-Rest**, **Data-in-Motion**, or **Data-in-Use** from the view vector menu.

Select graphical views

Select from the default graphical views to display incidents in configurations that can be understood at a glance.

Use these views to get ideas on how to display your incidents graphically.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click the **Group Detail** or **Summary** icons and review the results.

Copy views to users

Copy views that display configurations to groups of users who will find them useful.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **My Views**.
- On your McAfee DLP appliance, select **Incidents** | **My Views**.

2 Select one or more checkboxes.

3 From the **Actions** menu, select **Copy View to Users** and select one or more user groups.

4 Click **Apply**.

The warning appears: **This operation will overwrite views with the same name for the selected users if it exists**. If you want to continue, click **OK**.

Delete views

Delete views if their settings do not display incidents in useful configurations.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **My Views**.
- On your McAfee DLP appliance, select **Incidents** | **My Views**.

2 Select one or more checkboxes.

3 From the **Actions** menu, select **Delete**.

Customizing dashboards

Dashboards can be customized to expand the display area, list more incidents, or display additional attributes that are hidden by the default configuration.

Expand dashboard displays

Expand dashboard displays by collapsing or expanding the navigation pane. The size of the display and navigation panes can be reconfigured.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.
2 Double-click the vertical separator between the incidents and the navigation pane.
3 Repeat to restore.
4 Drag the separator to change the size of the panes.

Add rows to the dashboard

Add rows to the standard number displayed on dashboards (25 per page) by selecting a number on the **Columns** page.

Viewing a large number of incident rows at one time (1,000 or more) could cause an HTTP REQUEST timeout.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.
2 Click the **Columns** icon.
3 Select a number from the **Incidents per page** drop-down menu.
4 Click **Apply**.

Configure dashboard columns

Configure dashboard columns to modify the display of attributes of an object by selecting different columns from the **Columns** page.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.
2 Click the **Columns** icon.

3 On the **Table Columns** page, under **Selected**, select a column.

Reposition the order of the columns by using the **Move** buttons. Expand your dashboard if you cannot see them.

4 Click **Apply**.

Add a match string column

Add match string columns that reflect the content detected by a search or rule. Because match strings do not relate to all incidents, the column that contains them is not displayed by default.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click the **Columns** icon.

3 On the **Table Columns** page, under **Available**, select **MatchString** and click **Add**.

MatchString can only be applied to **Data-in-Motion** and **Data-at-Rest** incidents.

4 Click **Apply**.

Controlling dashboard settings

Changing dashboard settings can control how many incidents are reported at once, and how they are delivered to the dashboard.

You can configure throttling to control the number of incidents reported to the dashboard for the best possible system performance.

Encrypt incidents

Incidents are encrypted to prevent exposure of their contents, but you can choose to encrypt all of the information stored in the system.

Encryption is part of the initial setup of the system. When encryption is enabled, two significant components (subject and matchstring) that might contain PII (personally identifiable information) are encrypted before storing to the database. They are decrypted before displaying on the dashboard.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Settings**.
- On your McAfee DLP appliance, select **Policies** | **Settings**.

2 Select the **Encrypt Sensitive Incident Data** checkbox to encrypt all incidents found.

3 Select the **Encrypt Capture Data** checkbox to encrypt the entire capture database.

Selecting this option might impede performance.

4 Click **Save**.

Configure throttling to limit incidents reported

Configure throttling to limit the number of incidents reported to the dashboard. This helps to manage resources that are being consumed during that process.

You can set throttling to report between 1 and 9,999 incidents in a time frame that is between10 and 3600 seconds. Throttling is enabled by default; to report all incidents, deselect the **Enable Throttling** checkbox.

The throttling parameters *Time Duration* and *Number of Incidents* are global and applicable for all rules in the system. When throttling is enabled, if any rule triggers more incidents than specified in throttling parameters in the specified time duration, all extra incidents from that time duration will be suppressed.

Incident throttling is not supported for McAfee DLP Endpoint events.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Settings**.
   - On your McAfee DLP appliance, select **Policies** | **Settings**.

2 Under **Configure Throttling Parameters**, leave the **Enable Throttling** checkbox selected.

3 Type in the maximum **Number of Incidents** to be reported.

4 Type in the maximum **Time duration** in seconds.

5 Click **Save**.

Troubleshooting dashboard incidents

If incidents are being generated by McAfee DLP products but do not appear on the dashboards, make sure all requirements are met.

Table 15-3 Troubleshooting tips

Requirement	Task
Policies must be activated.	In the **Policy** tab, check the **State** column.
A time frame must be set.	In the **Filter by** frame, check the **Timestamp**.
Systems must be up.	In the **System** tab, check the **Health** icons.
Systems must be processing data.	In the **System** tab, click the **Statistics** icon.
Previous incident configurations must be released.	In the **Filter by** frame, click **Clear All**.
Capture filters must be configured correctly.	In the **System** tab, check to see what **Capture Filters** are active.
Data must be accessible (McAfee DLP Monitor).	In the **Capture** tab, enter a common keyword.
Scans must be set up, or data must be registered (McAfee DLP Discover).	In the **Classify** tab, verify that **Scan Operations** are active; on the **Policies** tab, check for **Registered Documents**.
Events must be generated (McAfee DLP Endpoint).	In the **System** tab, check **Endpoint Configuration**	**Manage Endpoints** to verify that an Endpoint policy is being generated.

Generating reports

Reports contain the content of the incidents and events displayed on the dashboard. They are available in PDF, HTML, or CSV format.

If you want to save the dashboard settings, save a **View** instead.

There are limitations on size and number of incidents supported in reports. The maximum size of reports is 5 MB; an incident that is exported cannot be saved if it is larger than that.

CSV reports must not exceed 150,000 incidents.

Create PDF reports

Create PDF reports up to 5 MB in size by selecting the format from the **Options** menu on the **Incidents** dashboard. Up to 5,000 incidents can be reported.

Reports from the **Incident Details** page include one incident unless the **List** button is selected.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select one of these options:
- From the **Incidents** dashboard, click **Options** and select the PDF report format.
- From the **Incident Details** page, click the PDF icon.

3 Allow some time for the report to generate.

4 **Open** or **Save** the report.

5 Click **OK**.

Create HTML reports

Create HTML reports up to 5 MB in size by selecting the format from the **Options** menu on the **Incidents** dashboard. Up to 5,000 incidents can be reported.

Reports from the **Incident Details** page include one incident unless the **List** button is selected.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select**Incidents** .

2 Select one of these options:
- From the **Incidents** dashboard, click **Options** and select the HTML report format.
- From the **Incident Details** page, click the HTML icon.

3 Allow some time for the report to generate.

4 **Open** or **Save** the report.

5 Click **OK**.

Create CSV reports

Create CSV (comma-separated values) reports by selecting one or more incident checkboxes on the **Incident Listing**, then select **Export CSV** from the **Options** button.

CSV reports can only be generated from **List**. Only PDF or HTML reports are supported in the **Summary** and **Group Detail** displays.

If you are on the **Incident Details** page when you decide to create a report, click the **List** button to return to the previous view.

For the CSV report type, there is no maximum number of incidents or maximum report size. The report will launch in spreadsheet format if you have Microsoft Excel installed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select one of these options:

- From the **Incidents** dashboard, click **Options** and select the CSV report format.
- From the **Incident Details** page, click **List** and select the checkbox of a single incident, then click **Options** to select the CSV report format.

3 Allow some time for the report to generate.

4 **Open** or **Save** the report.

5 Click **OK**.

Schedule reports

Schedule reports of incidents to run on a regular basis.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Click the **Save View** (Disk) icon.

3 In the **View Name** field, enter a name for the report.

4 From the **Set Owner** menu, select the report owner.

5 Select the **Schedule Reports** checkbox.

Reports and Views share the same interface. Select **Set as Home View** to set the current dashboard configuration as a view.

6 Select a checkbox to choose a report type.

7 Configure time and schedule settings.
   a In the **Start Date** field, enter the date to begin running the scheduled report.
   b In the **End Date** field, enter the last date that you want the report to run.
   c Configure the time of day to run the report.
   d Select one of the **Run Schedule** options to specify the frequency of the report.
      The scheduled report ignores any **Timestamp** filters set on the **Incidents** page. The frequency of the report also determines the date range of incidents included in the report.
      Example: If you select **Weekly on** and specify **Wednesday**, the report runs every Wednesday and includes incidents from the past seven days.
8 [Optional] Set up notification.
   By default, the email address of the user who is logged on is automatically entered in the **From** field.
   a Type a different or additional email address in the **From** field.
   b Type one or more email recipients in the **To** field.
   c Type an email subject in the **Subject** field.
   d Enter a message in the **Message** field.
9 Click **Save**.

Add titles to reports

Add a company name or other identifying information to a report.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
   - On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.
2 Click the **Configure** link for the McAfee DLP Manager being used to create the report.
3 Scroll down to **Company Information (for reports)**.
4 Type in a company or organization name.
5 Click **Update**.

Add custom logos to reports

By default, a report contains the McAfee logo. You can specify a custom logo to use instead.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
   - On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.
2 Click the **Configure** link for the McAfee DLP appliance used to create the report.
3 Scroll down to **Company Information (for reports)**.

4 Next to **Custom Logo**, select **Custom**.

5 Click **Browse** and navigate to the custom logo.

6 Click **Update**.

Typical scenarios

Incidents can be viewed, sorted, filtered, assigned to cases, and used in reports to display the most significant violations found by McAfee DLP systems. Some typical use cases follow.

Tasks

- *Find policy violations by user* on page 255
  If you have a lot of incidents to sort through, it might be hard to find the ones that are related to a particular user.
- *Find high-risk incidents* on page 256
  When you have a high volume of violations to search through, it might be difficult to find the most significant ones.

Find policy violations by user

If you have a lot of incidents to sort through, it might be hard to find the ones that are related to a particular user.

This case helps you to find policies that were violated by a user by keying on attributes that identify the user.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select **UserID**, **UserName**, or **UserEmail** and **equals**, then type the user's ID, name, or email address in the value field.

If you don't have exact information but want to guess at the identity of a sender or recipient, select the **Sender** or **Recipient** filter, add a **like** or **not like** condition, and type a string that might match some characters in the user's ID, name or email address.

3 In the **Group by** menu, the policies violated by the user are listed.

- Click a policy to display the incidents generated by its rules.
- Click an incident and select **Details** to determine the policy and rule that generated it.

If the policy did not generate incidents, it is not listed.

4 From the **Filter by** menu, select a time from the **Timestamp** sub-menu.

5 Click plus to add a filter.

6 Click **Apply**.

Find high-risk incidents

When you have a high volume of violations to search through, it might be difficult to find the most significant ones.

This case helps you to filter your results to display only the most significant incidents.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 From the **Filter by** | **Timestamp** menu, select a time frame.

3 Click **+** to add another parameter, then select **Severity** | **equals** and type a number from 1 to 5. Alternatively, click **?** and select from the **Severity** pop-up menu.

4 Click **Apply**.

The incident list displays items of the selected severity.

16 Case management

Case management allows users to collaborate in the resolution of related incidents.

Contents

- *Managing cases*
- *Updating cases*
- *Customizing cases*
- *Typical scenario*

Managing cases

Cases are used to manage incidents through stages of resolution. When a case is resolved, it is closed.

When significant incidents are found and reported by the McAfee DLP system, they generally have one or more attributes in common. Assigning incidents with common properties to a single case allows users to collaborate to resolve them more quickly. Each staff member involved can focus on a single aspect to advance the resolution of the case.

For example, a case that contains emailed evidence might be assigned to members of a legal team, who might develop it so that it can be used in court. Each member of that team might add notes and citations, change status and priority, notify stakeholders, or redirect the case to another user who might be able to add information.

Case dashboards display information based on organizational responsibilities. For example, Human Resources personnel might see Acceptable Use violations, but not SOX compliance issues.

Add, delete, or save cases

Add or delete cases to keep your case list up to date, and save the case information you will need in the future by exporting it.

Tasks

- *Add new cases* on page 258
  Add new cases to resolve related incidents.
- *Assign incidents to existing cases* on page 258
  You can add information to existing cases by adding incidents as they are detected over time.
- *Delete incidents from within cases* on page 259
  Delete incidents from within cases if they are resolved or no longer relevant to the case.
- *Delete cases from the case list* on page 259
  Delete cases from the **Case List** if they are resolved or no longer useful.
- *Export cases* on page 259
  Export cases to save single or multiple cases in .zip archives. When completed, the archives are displayed on the **Exported Cases** page.

Add new cases

Add new cases to resolve related incidents.

You can populate the new cases by adding one or more incidents immediately, or by adding incidents as they are detected over time. Select one or more from the **Incidents** dashboards, or add them one by one from within their **Incident Details** pages.

Up to 100 incidents can be added to a case at one time.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
   - On your McAfee DLP appliance, select **Case** | **Case Management**.
2 From the **Actions** menu, select **New Case**.
3 Complete the selections on the page, then click **Apply**.

Assign incidents to existing cases

You can add information to existing cases by adding incidents as they are detected over time.

To assign incidents to cases that contain related incidents, select one or more from the **Incidents** dashboards, or add them one by one from within their **Incident Details** pages.

Up to 100 incidents can be added to a case at one time.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
   - On your McAfee DLP appliance, select **Incidents**.
2 Select one or more incident checkboxes.
3 Click **Assign to Case**, then select **Existing Case** from the sub-menu.

4 On the **Case List** page, choose a case on the list, then click its **Assign** link.

If you cannot see the **Assign** column, expand your dashboard.

The **Case Details** page appears.

5 Complete the **Case Details** page, then click **Apply**.

Delete incidents from within cases

Delete incidents from within cases if they are resolved or no longer relevant to the case.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 In the **Case List**, click **Details** for the case from which incidents are to be deleted.

3 Select the incidents to be deleted.

4 From the **Options** menu, select **Delete**.

Delete cases from the case list

Delete cases from the **Case List** if they are resolved or no longer useful.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 In the **Case List**, select the cases to be deleted.

3 Delete cases in one of two ways.

- From the **Actions** menu, select **Delete**.
- In the **Delete** column, click the trash can icon.

Export cases

Export cases to save single or multiple cases in .zip archives. When completed, the archives are displayed on the **Exported Cases** page.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 In the **Case List**, select one or more case checkboxes.

You can export a single case, or include several cases in the same archive.

- Select a single case and click **Export**.
- Select one or more cases, then select **Export Selected Cases** from the **Actions** menu. In the **Proceed to export?** pop-up, click **OK** or **Cancel**.

The archive containing the case(s) appears in the these file lists:

- **ePolicy Orchestrator** — **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Exported Cases**
- **Your McAfee DLP appliance** — **Case** | **Exported Cases**

Manage case permissions

There are two levels of case permissions: administrators can assign case permissions to groups of users whose roles require case access; and users who have been given case permissions can manage access to specific cases.

Administrators have permissions to assign, manage, export, and delete case permissions to user groups, and they can also override permissions assigned to individual users. Case users can assign read, write, and delete permissions for a case to other groups or individual users.

Access to the case permissions page requires at least case-level read and delete permissions, plus task-level management permission assigned by an administrator. If write permission is assigned on the case management page, read access is included, even if that permission is not explicitly assigned.

The multi-level case permissions system makes it possible to restrict case access to users who are tasked with a particular case or type of case. For example, permissions can be set so that members of an *Operations* group cannot view confidential personnel cases that are managed by members of a *Human Resources* group.

If the user is not authorized to complete this task, the **Permission** menu item is disabled.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
   - On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Select a case and click **Details**.

3 Select **Options** | **Permissions**.

4 Select the **Read**, **Write**, or **Delete** checkboxes corresponding to the assignment of the case to users and groups.

   Users who create cases are automatically allocated all three permissions — but if a case owner is changed, permissions are lost.

5 Click **Apply**.

Global permissions take precedence over cases configured individually. If there is a conflict between permissions assigned under an individual case and those that are assigned globally, global group permissions take precedence.

- In ePolicy Orchestrator, global permissions are set under **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Groups** | **Details** | **Task Permissions**.
- On your McAfee DLP appliance, global permissions are set under **System** | **User Administration** | **Groups** | **Details** | **Task Permissions**.

When **Write** permission is assigned, **Read** permission is implicit.

How user permissions might be assigned

John has been given read access, so case information is displayed on his home page. But because his permission is restricted to **Read**, he will not see the **Apply**, **Save**, **Delete**, or **Assign** buttons.

Sheila has been given responsibility for developing court cases, so she has been given **Read** and **Write** but not **Delete** permissions. Because of the nature of legal actions, only her manager can see the **Delete** button on his console.

Updating cases

As you gather more information about a case, you can develop it gradually by adding incidents, defining different aspects of it, and recording updates until you are able to resolve it.

Change ownership of a case

Change ownership of a case to give primary responsibility for resolution to a specific user group.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
   - On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Click **Details** for a case.

3 From the **Owner** menu, select a user group.

Select the **Notify Owner** checkbox to send email notification of case updates.

4 Click **Apply**.

Change status of a case

Change the status of a case to indicate its stage of resolution.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
   - On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Click **Details** for a case.

3 From the **Status** menu, select a new status.

4 Click **Apply**.

Change the priority of a case

Change the priority of a case as it moves through stages of resolution.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
   - On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Click **Details** for the case.

3 From the **Priority** menu, select a new priority.

4 Click **Apply**.

Change the resolution stage of a case

Change the resolution state of a case if its condition has changed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Click **Details** for a case.

3 From the **Resolution** menu, select a new stage.

4 Click **Apply**.

Add notes to a case

Add notes to a case to add comments that might help to resolve it.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Click **Details** for a case.

3 In the **Add Notes** text box, type a comment.

4 Click **Apply**.

Customizing cases

Customizing cases will help you to resolve them more quickly.

You can add custom fields to sort case incidents by attribute, or add columns on the Case List dashboard to display the most useful information. Notifications and periodic reminders for stakeholders can also help to expedite resolution.

Add or remove attachments to cases

Add or remove attachments to cases that might provide additional information for resolution.

Before you begin

The **Case List** should display at least one case.

Case attachments can be added or removed only by users who have case-level write permission. Viewing them requires both task-level and case-level read permissions. If those permissions are not assigned, the **Case Attachments** option is disabled.

No more than 50 attachments can be uploaded, and attachment size cannot exceed 50 MB.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Select a case and click **Details**.

3 Scroll down to the list of incidents contained in the case.

The **Case Attachments** window appears, and attachments that have already been added are listed.

4 From the **Options** menu, select **Case Attachment**.

- If you want to remove attachments, select the appropriate checkboxes and click **Remove Attachments**.
- If you want to add attachments, click **Browse** and locate the attachment, then click **Upload Your File**.

5 Click **Back** to return to the case.

Add or remove custom case attributes

Add or remove custom case attributes that will give them a common context.

Before you begin

The **Case List** should display one or more cases.

For example, the added attributes might be additional criteria that must be met before the cases in your list can be resolved.

Case attributes can be added or removed only by users who have case-level write permission. Viewing them requires both task-level and case-level read permissions. If those permissions are not assigned, the **Customize Case Config** option is disabled.

No more than ten comma-separated attributes can be added, but spaces within them are supported. However, attributes cannot exceed a total of 80 characters.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 From the **Options** menu, select **Custom Case Config**.

- If you want to add attributes, type comma-separated values and click **Apply**.
- If you want to notify or remove notification of case stakeholders, select **Notify Submitter** or **Notify Owner** checkboxes and click **Apply**.
- If you want to notify the case owner of new or updated permissions, define the notification time frame, select the appropriate options, and click **Apply**.

Customize Case List columns

Customize columns on the **Case List** to display the information that is most useful for resolving cases.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 From the **Options** menu, select **Customize Columns**.

3 Select a column header from the **Available** menu and click **Add** to move it to the **Selected** menu.

4 Click the **Move** button to move **Selected** column headers up or down.

On the **Case List** page, selecting the up and down arrows moves columns from left to right.

If you cannot see the **Move** controls, expand your dashboard.

5 Click **Apply**.

Customize case notifications

Customize case notifications by setting up periodic reminders that keep stakeholders informed as the case develops. Notification might include any change in case permissions.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Select one or more case checkboxes.

3 From the **Options** menu, select **Customize Case Config**.

4 Select **Notify Submitter** or **Notify Owner** checkboxes when the case is updated.

5 Select the options to define periodic or permissions parameters, if appropriate.

6 Click **Apply**.

Notify stakeholders of case updates

Keep case stakeholders informed about developments in a case by notifying submitters or owners each time it is updated.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Case Management**.
- On your McAfee DLP appliance, select **Case** | **Case Management**.

2 Click **Details** for a case.

3 Check **Notify Submitter** or **Notify Owner**.

4 Click **Apply**.

Notifications are sent the next time the case is updated.

Typical scenario

Cases can be used to resolve groups of related incidents. A typical use case follows.

Resolve credit card violations using a case

If you collect credit card violations in a case, you can resolve *Payment Card Industry* violations in a single operation.

Before you begin

A privacy policy that contains credit card rules must be installed and activated. When the rules run, violations are found and reported to the **Incidents** dashboard. They can then be added to the case.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Find credit card violations on the dashboard, then select one or more incident checkboxes.

3 Click **Assign to Case**, then select **New Case** or **Existing Case** from the sub-menu.

- If you select **New Case**, complete the **Case Details** page, and click **Apply**.
- If you select **Existing Case**, choose a case on the list, click its **Assign** link, complete the **Case Details** page, and click **Apply**.

If you cannot see the **Assign** column, expand your dashboard.

4 From the **Options** menu, select **Customize Case Config** and add attributes that might help you to put each incident into a customized context.

For example, you might add a source field that allows you to type a note on the **Case Details** page about the origin of the incident.

5 From the **Options** menu, select **Customize Columns** and rearrange the dashboard to display only the most useful attributes of the object found.

6 From the **Options** menu, select **Customize Case Config** and select **Owner** and **Submitter** checkboxes to keep the stakeholders updated on the progress of the case.

7 On the **Case List**, open the credit card violation case and examine each of the incidents in the case to find out what they have in common.

8 Update the **Notes** field on the **Case Details** page each time a new violation is added to the case, or whenever you or your collaborators find another piece of the puzzle.

By cooperating in developing the case, you and your colleagues can act as a team to find out how credit card violations are generated, devise a process to prevent more of them, and if the data loss is not accidental, build a legal case against the perpetrators.

17 Searching captured data

The McAfee DLP interface supports basic and advanced searches. You can save searches as rules to use the same parameters again.

Contents

- *How McAfee DLP handles searching*
- *Search basics*
- *Using logical operators in searches*
- *Using keywords in searches*
- *Using concepts in searches*
- *Search based on network parameters*
- *Search based on file parameters*
- *Typical scenarios*

How McAfee DLP handles searching

The capture engine classifies and parses data by content type. Each object is made up of many attributes that are stored with it in the databases.

These objects are retrieved by building searches. Creating a search is similar to creating a rule, and you can save a search as a new rule. Performing searches on captured data can help you determine if new rules are needed or if existing rules should be refined. You can learn to form searches by examining some of the standard rules under the policies listed under the **Policies** tab. The parameters used in existing rules might suggest combinations that are useful in finding the data you need.

Searching is role-based and requires that the correct permissions are set for the user attempting to perform the search.

The amount of captured data saved in the database is dependent on the available disk space. If the database has reached its capacity, the earliest data is removed. Time-based wiping can be configured from 30–180 days.

Distributed searching

Searches that are distributed to more than one McAfee DLP appliance are handled through McAfee DLP Manager.

Although distributed searches default to **All Devices**, the **Devices** button on the **Advanced Search** page supports searches on specific McAfee DLP devices.

Large-scale searches

Searches that take over 60 seconds to process run in background mode. When the search is complete, the user who is logged on is notified by email.

Although distributed searches default to **All Devices**, the **Devices** button on the **Advanced Search** page supports searches on specific McAfee DLP devices.

Number of results supported

The search engine imposes limitations on the number of search results supported by McAfee DLP.

The search engine is designed to retrieve no more than 100,000 results at a time. If this limit is exceeded, match strings will not be retrieved, and hits on substrings might return overly broad results.

The dashboard incident list is limited to 5,000 results, but up to 150,000 incidents can be exported via CSV. Export from dashboard is limited to 5K. If your search results exceed this number, narrow your query and repeat the search.

Archive handling

When archived files are captured, they are opened and their contents are analyzed by the indexer.

The search engine finds, extracts, and evaluates content in .zip, .gzip, and .tar archives, but only if the compressed file type is identified in the query.

The following compressed file types are supported:

- GZIP
- ZIP
- TAR
- StuffIt
- BinHex
- Compress
- MS Cabinet
- EncryptedZip
- RAR
- TNEF

Case insensitivity

Case sensitivity is ignored by the search engine.

For example, if a query is defined in ALL CAPS, the indexer retrieves and reports the matching content whether it is in uppercase or lowercase.

Microsoft Office 2007 anomalies

The indexer ignores certain Microsoft Office attributes because of the way those applications handle fonts, colors, macros, and page definition.

- If two dictionary words are merged together, the merged word will not be found. For example, `American` and `Recovery` are two dictionary words. If they are merged into the word `AmericanRecovery`, they will not be found.
- If a word in a Microsoft Office document has different fonts and colors, the word will not be read as a whole and will not be found. For example, if all the letters in the word `Recovery` are of different fonts and colors, it will not be found.
- If a word continues across two different pages, it will not be found. For example, if the word `Recovery` is spread across two pages (one page contains `Rec` and the second page contains `overy`), it will not be found.

- Words in documents that use special Microsoft Office font features like WordArt, SmartArt, and watermarks will not be found.
- Words present in macros in Microsoft Office documents, and headers and footers in PowerPoint and Excel, will not be found.

Negative searches

The database cannot recognize queries that consist entirely of negative terms because a query containing only words that are *not* to be found is instructing the search engine not to search.

For this reason, some scope of data within which the term will *not* be found must be defined.

Proper name treatment

The indexer treats proper names like keywords, so it is not necessary to capitalize them.

Parts of speech excluded from capture

The capture engine excludes common parts of speech to prevent insignificant results from being stored and retrieved.

For example, the following parts of speech are ignored by the indexer:

- `a`
- `and`
- `this`
- `therefore`
- `else`
- `while`
- `with`

Users can deploy the **Stop-Word** concept to define words the capture engine should ignore.

Special character exceptions

Certain special characters are not supported in queries. Words that include non-alphabetic characters, such as numbers or spaces, are supported only if they are identified in an Exact Search.

Table 17-1 Characters that cannot be used in queries

Character	Description
.	period
;	semicolon
|	pipe
`	back tick
<>	less than/greater than
( )	parentheses
\ \\	backslashes
/>]]>	markup
*	control characters
/	escape characters

Word stemming

The capture engine supports word stemming to return words related to a query, but imposes restrictions to retrieve the most significant results.

Do not use tildes (~) or asterisks (*) to retrieve words related to a word stem.

If a plural or gerund of a complete word used in a search is found, the result is reported as if it were a word stem. For example, searching for *basket* to retrieve *basketball* will not work, but it will return *baskets*. Similarly, searching for *run* will return result *running*.

Word stemming takes precedence in exact searches. For example, when you enter a query like **Keywords** | **Exact Match** | **information**, the keyword will be stemmed to "inform", which will return all strings that contain that stem word. To prevent word stemming in such a case, include additional words in your query.

You can use word stemming with logical parameters and additional parameters to focus a query. For example, use **Keyword** | **expression** with the following expression to find documents containing the word *Confidential* that are also marked EITHER *Eyes Only* or *Do Not Distribute* OR contain variations of the words *secret* or *secure*.

Confidential + (("Eyes Only" || "Do Not Distribute") || (secret))

The word stem in this example returns related words, such as secrets or secretive. Incomplete or partial words are not recognized.

Search basics

You can use the following tasks to help you to build successful queries.

Tasks

- *Add or delete parameters* on page 271
  Add or subtract McAfee DLP parameters that correspond to database object attributes by clicking **+**, **-**, or **X** buttons on the search, rule, template, case, or capture filter pages.
- *Retrieve data from directory servers* on page 271
  If a directory server is registered to McAfee DLP Manager, you can retrieve data from it by user name, group, city, country, or organization.
- *Get search details* on page 272
  The stages of each search are recorded and displayed in the **Search Details** window.
- *View search results* on page 272
  View the objects that matched a search.
- *Stop searching* on page 272
  You can stop searches that are running by using the **Abort** function.
- *Set up notification for backgrounded queries* on page 273
  Searches that take over 60 seconds automatically run in background mode, but when results are available, an email notification is sent to the address you provide.
- *Clone searches* on page 273
  If you want to use the same search repetitively, you can clone it so that you can repeat the process without re-selecting all of your parameters.

Add or delete parameters

Add or subtract McAfee DLP parameters that correspond to database object attributes by clicking **+**, **-**, or **X** buttons on the search, rule, template, case, or capture filter pages.

The following procedure uses the **Advanced Search** page as an example.

Task

1. Select a page in the user interface that displays configurable parameters, using one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2. Open any category.
3. Click **+** to define a new parameter.
4. Select either of the following methods to delete parameters:
   - In category frames, click **-** to delete a single parameter.
   - Beside category names, click **X** to delete multiple parameters.

Retrieve data from directory servers

If a directory server is registered to McAfee DLP Manager, you can retrieve data from it by user name, group, city, country, or organization.

> **Before you begin**
>
> An Active Directory or OpenLDAP server must be registered to McAfee DLP Manager.

Task

1. Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2. Open the **Source/Destination** category.
3. Select a **User** parameter.

   User name, group, city, country and organization parameters are supported on directory servers.

   For example, select **User Organization**.
4. Select **sender is any of** or **sender is none of**.

   Recipient values are not supported.
5. Click **?** and select a directory server from the menu.

   The **AD pop-up** window appears.
6. Type a pattern into the search field, or click **Find**.

   If no pattern is entered, a list of user values found in the directory server appears.
7. Click one or more values and click **Apply**.

   For example, select the **Contractors** organization.

   The **Advanced Search** page reappears.

8 Add more parameters that will narrow the search.

For example, add email addresses that contractors might be using to distribute proprietary information, and an *Engineering Drawing* content parameter that contains intellectual property.

9 Click **Search** or **Save as Rule**.

Get search details

The stages of each search are recorded and displayed in the **Search Details** window.

This display is different from search **Results**, which are displayed on the McAfee DLP Manager dashboard.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Search List**.
- On your McAfee DLP appliance, select **Capture** | **Search List**.

2 Click the **Details** link.

The stages of the search process are displayed.

View search results

View the objects that matched a search.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Search List**.
- On your McAfee DLP appliance, select **Capture** | **Search List**.

2 Click the **Results** link.

3 For more information on a match, click **Details**.

- If there is a user associated with the match, click the link next to **User ID** to view more information about the user.

  The user and group information displayed in search results contains some of the information shown in the incident **User Details** window. For example, Distinguished Name information for the group is not displayed. The search result does display the Security Identifier (SID), which uniquely identifies a user by associating the user with attributes such as domain name, location, department, and the group the user belongs to.

- If there is a file associated with the match, click the link in the **Content** area to open or download the file.

Stop searching

You can stop searches that are running by using the **Abort** function.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Search List**.
- On your McAfee DLP appliance, select **Capture** | **Search List**.

All searches are listed in chronological order by database searched.

2 Click **Abort** for the search you want to stop.

Set up notification for backgrounded queries

Searches that take over 60 seconds automatically run in background mode, but when results are available, an email notification is sent to the address you provide.

Click **My Profile** at the top of the page and type the email address.

If a search is aborted, no notification is sent.

After notification is set up, you must log out and log on to register the change — but you can configure the email client to prompt you when new email comes in.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration**.
- On your McAfee DLP appliance, select **System** | **User Administration**.

2 Click **Details** for the user.

3 Type an email address into the **Email** field.

4 Click **Apply**.

Clone searches

If you want to use the same search repetitively, you can clone it so that you can repeat the process without re-selecting all of your parameters.

You can clone the search, but get different results by modifying one or two parameters before clicking **Search** again.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 On the **Advanced Search** page, select search terms and click **Search**.

3 In the page header, click **Search List**.

4 Click **Clone Search**.

The **Advanced Search** page reappears, displaying the parameters entered for the previous query.

5 Click **Search** to restart the search, or modify parameters before clicking **Search** again.

Using logical operators in searches

McAfee DLP supports specific logical operators in queries.
All operators, including **Exact Match**, are case-insensitive. For example, if you search for a term in ALL CAPS, the system will return that in capital letters, initial caps, and lowercase letters.

In **Exact Match**, word stemming takes precedence. For example, if you search for *information*, the keyword will be stemmed to *inform*, which will return all strings that contain that stem word. Include additional words in your query to find the word to prevent stemming.

Word stemming queries do not require any notation. Do not use asterisks or tildes.

You can use an OR logical operator (`||` or `OR`) instead of a comma to construct a query. But you cannot use AND operators between URLs and email fields.

Logical operators supported in queries

Logical operator	Notation	Examples
AND	`+ &&`	`Confidential Restricted Secret`
		`Confidential AND Restricted AND Secret`
		`Confidential and Restricted and Secret`
		`Confidential + Restricted + Secret`
		`Confidential && Restricted && Secret`
OR	`or ||`	`Confidential OR Restricted OR Secret`
		`Confidential or Restricted or Secret`
		`(Confidential || Restricted) && Secret`
NOT	`- !`	`Confidential -Restricted -Secret`
		`Confidential !Restricted !Secret`
Word Stemming		`Confidential Restrict Secret`
Parentheses	`( )`	`Confidential AND (Restricted OR Secret)`
Exact Match	`" "`	`"Confidential and Secret"`

Examples of queries using logical operators

Build customized queries by using logical operators in McAfee DLP search fields.

Use the following examples to learn to construct keyword queries using the expressions and exact phrases fields.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Capture** | **Advanced Search.**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keyword** | **exact phrase** or **Keyword** | **expression**.

4 Enter a query using logical operators in the value field.

5 Click **Search**.

Compound queries that will produce the same results

confidential + "Eyes Only" OR "Do Not Distribute" -secret -security

Confidential "Eyes Only" || "Do Not Distribute" !secret !security

Complex query that adds grouping of search terms and use of word stemming

Confidential + (("Eyes Only" || "Do Not Distribute") || (secret))

This query finds documents containing the word *Confidential* that are also marked EITHER *Eyes Only* or *Do Not Distribute* OR contain variations of the words *secret*.

Using keywords in searches

Keywords can be used or excluded from searches.

Using keywords to find incidents

Keyword usage is determined by the properties of the language that is being used to query the capture database. Non-English keywords are considered exact phrases.

Use logical operators with exact phrases and keyword expressions to get the most relevant results.

Examples

Keyword inclusion

When keywords are used with the **contains all of** condition, spaces between words imply AND. For example, **Keywords** | **contains all of** | **Intel AMD NVidia**

When keywords are used with the **contains any of** condition, spaces between words imply OR. For example, **Keywords** | **contains any of** | **Intel AMD NVidia**

When keywords are used with the **exact phrase** condition, spaces between words are literal. For example, **Keywords** | **exact phrase** | **NVidia supports AMD and Intel platforms.**

Keyword exclusion

When keywords are used with the **contains none of** condition, results that contain the keyword are excluded; but negative searches are not supported, so some positive condition must first be specified. For example, **Keywords** | **contains any of** | **Intel AMD**. Another parameter can then be added to exclude a related keyword from the results. For example, **Keywords** | **contains none of** | **NVidia.**

Keyword expressions

If **Keywords** | **expression** is selected, queries using logical operators can be typed directly into the value field. For example, the following expression finds one of the expressions in the first set of parentheses, but neither of the expression in the second set of parentheses. For example, `(Intel || AMD) !(Nvidia && ATI)`.

Keyword exact phrases

You might use an exact phrase keyword search to find specific UTF-8 characters. For example, select **Keywords exact phrase** and paste `<characters>` into the value field.

Find incidents using keywords

Find significant incidents and violations in network data by using keywords in queries.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Enter keywords in one of two ways:

- On the **Basic Search** menu, type one or more keywords, and click **Search**.
- On the **Advanced Search** page, open the **Content** category, type one or more keywords, and click **Search**.

Find incidents by excluding keywords

Exclude keywords from a query to keep from retrieving incidents that contain them.

An exclusion search could result in too many hits. Limit the query by adding more parameters.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**..
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keywords** | **contains none of** and enter one or more keywords in the value field.

4 Click **Search** or **Save as Rule**.

Find exact keyword matches

Find exact keywords or UTF-8 characters by using the **Exact Phrase** condition. With this condition, you can use logical operators to extend your query.

UTF-16 characters cannot be found using this feature.

Because search is case-insensitive, you need not capitalize the keywords. Do not add quotation marks and parentheses; they are added by the search engine.

In **Exact Match**, word stemming takes precedence. For example, if you search for *information*, the keyword will be stemmed to *inform*, which will return all strings that contain that stem word. Include additional words in your query to find the word to prevent stemming.

Word stemming queries do not require any notation. Do not use asterisks or tildes.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keywords** | **exact phrase** and type the keywords to be matched into the value field.

4 Click **Search** or **Save as Rule**.

Find non-English keywords

Find non-English keywords by using the **Exact Phrase** feature. Because the search engine supports the standard UTF-8 (UCS Transformation Format - 8-bit) encoding, you can find words using many different character sets, and you can extend your query by using logical operators.

Non-English searches must contain exact characters.

UTF-16 characters are translated to UTF-8, so pasting them into the value field will not work.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keywords** | **exact phrase** and paste the keywords and logical operators into the value field.

4 Click **Search** or **Save as Rule**.

Build keyword expressions with logical operators

You can build complex keyword queries using logical operators using the **keyword expressions** condition. You can also add regular expressions to the value field to find text patterns.

Logical operations can also be used with the **exact phrases** condition.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keywords** | **expression** and enter keywords and logical operators in the value field.

4 Click **Search**.

Using concepts in searches

Content and session concepts can be used to find data patterns and content in data being exchanged between clients and servers.

Find incidents using content concepts

Content concepts are collections of alphanumeric data that are relevant to a single issue, so they can be used efficiently to find related incidents.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Concept** | **is any of** and click **?**.

   The **Concepts** window opens.

4 Open categories and select concept checkboxes.

5 Click **Apply**.

6 Click **Search**.

Build concept expressions with logical operators

Content concepts are collections of data relevant to a single issue, so they are useful for finding related incidents. If you add an **expressions** condition, you can narrow the concept query by using logical operators.

To match more than one pattern in a single search, enter concepts in the **Value** field using the `concept:ConceptName` format with logical operators.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Concept** from the **Element** menu and **expression** from the **Condition** menu.

4 Enter a compound concept query using logical expressions in the **Value** field.

   The logical expressions supported are `+ AND - OR ! NOT` .

5 Click **Search**.

   For example, the expression `concept:VISA +concept:MASTERCARD !concept:DISCOVER ! concept:AMEX` finds credit card numbers that are in Visa or MasterCard format, but not Discover or American Express.

Exclude concepts to filter results

When you exclude content concepts from a query, you can focus results by filtering out irrelevant collections of data.

Example: If you wanted to find credit cards using any possible numbering pattern except American Express, you could select the AMEX concept to exclude those results from a general payment card query.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Click a policy to open it and select a rule that retrieves too many results.

Because a rule is a search that has been saved, this procedure also relates to an over-broad search.

3 Open the **Content** category.

4 Click on **+** to add a parameter to the rule.

5 Select **Concept** | **is none of** and click **?**.

The **Concepts** pop-up menu appears.

6 Open one or more concept categories.

7 Select one or more concepts.

8 Click **Apply**.

9 Click **Save**.

Search based on network parameters

Use network parameters, such as IP address, port, and time to find captured data.

Tasks

- *Search using time parameters* on page 280
  Because of the volume of data captured, it is essential to define a time frame before searching. Every file is time-stamped when it is added to one of the McAfee DLP databases.
- *Search by port* on page 282
  Search by port to identify incidents by source, destination, or in both directions.
- *Search by port range* on page 282
  Search by port range to identify incidents in a type of traffic by source, destination, or both.
- *Search by excluding ports* on page 283
  Exclude ports from a query to prevent incidents using them from appearing in search results.
- *Search by using protocols* on page 284
  You can identify a specific type of traffic by using protocols as search qualifiers.
- *Search by excluding protocols* on page 284
  Exclude protocols from a query to prevent incidents using them from appearing in search results.
- *Find IP addresses in incidents* on page 285
  Find IP addresses in incidents by range, by subnet, or by exclusion.

Search using time parameters

Because of the volume of data captured, it is essential to define a time frame before searching. Every file is time-stamped when it is added to one of the McAfee DLP databases.

Objects are time-stamped in UTC Universal Coordinated Time at the moment they are captured in network traffic, found in file systems or databases, or generated as endpoint events. McAfee DLP systems do conversion between local and global time automatically.

For this reason, it is essential to set time frames for searches or rules, and to remember the date of installation of a McAfee DLP appliance. The system cannot retrieve results that have not yet been found.

If a time frame is set as a filter, any results reported as the result of a search or rule will be constrained to that time frame. The filter must be cleared before the results outside of that time frame can be viewed.

Tasks

- *Search for files by global time (GMT)* on page 281
  When you set a **Date/Time** parameter in a search or rule, local time is automatically converted to Greenwich Mean Time (GMT). This default allows you to find files that might be time-stamped at or near the same time globally by creation, modification, or last accessed times.
- *Search in a relative time frame* on page 281
  The search engine is able to locate files that are time-stamped within a relative time frame.
- *Search by file creation time* on page 281
  Search for files that were created at a particular time.
- *Search by file last modification time* on page 282
  Search for files by the last time they were modified.

Search for files by global time (GMT)

When you set a **Date/Time** parameter in a search or rule, local time is automatically converted to Greenwich Mean Time (GMT). This default allows you to find files that might be time-stamped at or near the same time globally by creation, modification, or last accessed times.

The date and time set on your DLP appliances is determined by the local time zone in which they were installed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Date/Time** category and select **File Creation Time**, **Last Modification Time**, or **File Last Accessed Time**.

3 Select an approximate time from the **before/between/after** menu.

Select **between** to set both **before** and **after** delimiters.

4 From the calendar icon, select a date, and set hour, minute and second times with the thumbwheel menus.

5 Click **Search** or **Save as Rule**.

Search in a relative time frame

The search engine is able to locate files that are time-stamped within a relative time frame.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Date/Time** category.

3 Select **File Creation Time**, **File Last Accessed**, or **Last Modification Time** and **between** then click the calendar icon to enter dates in the values field.

Select **before** or **after** to get closer to a specific time.

4 Select a time from the hour, minute and second menus.

5 Click **Search**.

Search by file creation time

Search for files that were created at a particular time.

The time zone of the McAfee DLP appliance determines the file creation time displayed.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Date/Time** category.

3 Select **File Creation Time** | **between** and click the calendar icon to enter dates in the values field.
Select **before** or **after** to get closer to a specific time.

4 Select a time from the hour, minute and second menus.

5 Click **Search**.

Search by file last modification time

Search for files by the last time they were modified.

The time zone of the McAfee DLP appliance determines the last modification time displayed.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Date/Time** category.

3 Select **Last Modification Time** | **between** and click the calendar icon to enter dates in the values field.
Select **before** or **after** to get closer to a specific time.

4 Select a time from the hour, minute and second menus.

5 Click **Search**.

Search by port

Search by port to identify incidents by source, destination, or in both directions.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Port** | **source is any of** and enter a port number in the values field.

4 Click **+** to add a destination parameter.

5 Select **Port** | **destination is any of** and enter a port number in the values field.

6 Click **Search**.

Search by port range

Search by port range to identify incidents in a type of traffic by source, destination, or both.

This is especially useful when a specific type of traffic can be identified by a range. For example, the Solaris operating system often uses the 1000-1023 range.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Protocol** category.
3 Select **Port** | **source is any of** and enter a port number range in the values field.
4 Click **+** to add a destination parameter.
5 Select **Port** | **destination is any of** and enter a port number range in the values field.
6 Click **Search**.

Search by excluding ports

Exclude ports from a query to prevent incidents using them from appearing in search results.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Protocol** category.
3 Select **Port** | **source is none of** and enter a port number in the values field.
4 Click **+** to add a destination parameter.
5 Select **Port** | **destination is none of** and enter a port number in the values field.
6 Click **Search**.

Common port assignments

Well-known ports are commonly associated with specific types of traffic, and can be used to search network data.

The list in this table contains only a few of the well-known ports. IANA (Internet Assigned Numbers Authority) updates are online at http://www.iana.org/assignments/port-numbers.

Table 17-2 Common port assignments

Port number	Service
20/21	FTP
22	SSH
23	Telnet
25	SMTP
80	HTTP
110	POP3
123	NTP
143	IMAP

Table 17-2 Common port assignments *(continued)*

Port number	Service
144	NNTP
443	HTTPS
465, 587	SMTP-SSL
993	IMAP-SSL
995	POP3-SSL

Search by using protocols

You can identify a specific type of traffic by using protocols as search qualifiers.

For example, HTTP protocols might be identified to find incidents in web traffic, or FTP might be used to detect large quantities of data being transmitted.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Protocol** category.
3 Select **Protocol** | **is any of** and click **?**.

   The **Protocols** window appears.
4 Open categories and select protocol checkboxes.
5 Click **Apply**.
6 Click **Search**.

Search by excluding protocols

Exclude protocols from a query to prevent incidents using them from appearing in search results.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Protocol** category.
3 Select **Protocol** | **is none of** and click **?**.

   The **Protocols** pop-up menu appears.
4 Open categories and select protocol checkboxes.
5 Click **Apply**.
6 Click **Search**.

Find incidents related to geographic locations and web sites

Traffic to and from geographic locations or web sites might be reported in incidents.

Find incidents by geographic location

Find incidents sent to or from other countries by searching for geographic locations.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Open the regional pop-up menu in one of two ways:

- On the **Basic Search** menu, select **GeoIP Location**, click **?**, and select a region or country from the regional pop-up menu.
- On the **Advanced Search** page, open the **Source/Destination** category, select **GeoIP Location**, click **?**, select a region or country from the regional pop-up menu, and click **Apply**.

3 Click **Search**.

Find incidents related to web sites

Find incidents related to web sites by using URLs in queries.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **URL** | **is any of** and type one or more URLs.

4 Click **Search**.

Find IP addresses in incidents

Find IP addresses in incidents by range, by subnet, or by exclusion.

Tasks

- *Find IP addresses in captured data* on page 286
  Find IP addresses, a range of addresses, or a subnet containing IP addresses in captured data by using them in queries.
- *Find a range of IP addresses* on page 286
  Find incidents generated from specific IP addresses by entering them into value fields. Define multiple addresses or address ranges by separating them with commas or dashes.
- *Find IP addresses on subnets* on page 286
  Find subnetted IP addresses by using subnet masks in a query.
- *Exclude IP addresses from search results* on page 287
  Exclude single IP addresses or IP address ranges from search results to focus your query.

Find IP addresses in captured data

Find IP addresses, a range of addresses, or a subnet containing IP addresses in captured data by using them in queries.

Indicate a choice between two IP addresses by separating them with a comma (no spaces). You can search for single IP addresses, ranges, subnets, and addresses expressed in CIDR notation (see examples below).

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Find an IP address in captured data in one of two ways:

- On the **Basic Search** page, select **IP Address**, and type one or more IP addresses.
- On the **Advanced Search** page, open the **Source/Destination** category, select **IP Address**, and type one or more IP addresses.

3 Click **Search**.

Examples

192.168.3.225

10.1.0-10.0.1-255

172.16.1.1/24

Find a range of IP addresses

Find incidents generated from specific IP addresses by entering them into value fields. Define multiple addresses or address ranges by separating them with commas or dashes.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **IP Address** | **is any of** and enter the IP addresses, separated by a comma, in the value field. Identify IP address ranges by separating IP addresses with a dash.

192.168.1.244,172.25.3.100-172.25.3.199

4 Click **Search** or **Save as Rule**.

Find IP addresses on subnets

Find subnetted IP addresses by using subnet masks in a query.

Subnet searching is supported whether or not network and host portions of an IP address are standard classful IP (address fields separated into four 8-bit groups).

CIDR (Classless Inter-domain Routing) notation is supported.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **IP Address** | **is any of** and enter the subnetted IP addresses in the value field.

For example, for subnet mask 255.255.255.128, you can type `192.168.2.1/25`.

4 Click **Search** or **Save as Rule**.

Exclude IP addresses from search results

Exclude single IP addresses or IP address ranges from search results to focus your query.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search.**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **IP Address** | **is none of** and enter an IP address or range in the value field.

Add another parameter to narrow the focus of the query.

4 Click **Search** or **Save as Rule**.

Search for email

Email objects are stored in capture databases as separate tokens. Search for one or more components of an email address (user, host or domain names) to produce related results.

Because email attributes are captured, email can also be found by port, protocol, attachment, sender, recipient, cc, or bcc.

Email addresses or domain names that contain numbers are searchable only if they are in the addressing, subject, cc, or bcc fields. Only alphanumeric characters are supported in the body of email messages.

In rare cases, email addresses that are not present in SMTP mail might be displayed in strikeout mode in the highlighting on the dashboard.

Tasks

- *Find email by address* on page 288
  Find email sent or received by entering an email address in the value field.
- *Find email attachments* on page 289
  Find email attachments by searching for the protocols used to send them.
- *Find email by bcc* on page 289
  Find email by searching for email addresses on the **bcc**: line.
- *Find email by cc* on page 289
  Find email by searching for email addresses on the **cc**: line.
- *Find email by domain* on page 290
  Find email in discovered data by searching for domain names.
- *Find email by port* on page 290
  Find email by using searching for email types that are transported through well-known ports.
- *Find email by protocol* on page 290
  Find email by searching for the protocols used to send it.
- *Find email by sender or recipient* on page 291
  Find email sent or received by specific users by setting the **sender** or **recipient** condition on the **Email Address** menu, then entering an email address in the value field.
- *Find email by subject* on page 291
  Find email about specific topics by searching for the text contained in subject lines.
- *Find webmail by port* on page 291
  Find webmail by port by searching using well-known port 80 for web traffic in your query.
- *Find webmail by protocol* on page 292
  Find webmail by searching for communications that use port 80. Web traffic commonly uses port 80.
- *Find chat sessions* on page 292
  Find chat sessions by searching for chat content types. You can retrieve sessions lasting up to four hours.

Find email by address

Find email sent or received by entering an email address in the value field.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Enter an email address in one of two ways:

- On the **Basic Search** menu, type one or email addresses separated by commas (no space), and click **Search**.
- On the **Advanced Search** page, open the **Source/Destination** category, select **Email Address** | **is any of** and type one or more email addresses separated by commas (no space), then click **Search**.

Find email attachments

Find email attachments by searching for the protocols used to send them.

For example, HTTP_Webmail_Attach is used to find webmail attachments, and SMTP_Attach and POP3_Attach find email attachments.

Attachments larger than 50 MB cannot be reported.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Protocol** category and click **?**.
3 Open the **Mail Protocols** category.
4 Select one or more attachment types.
5 Click **Apply**.
6 Click **Search** or **Save as Rule**.

Find email by bcc

Find email by searching for email addresses on the **bcc:** line.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Source/Destination** category.
3 Select **Email BCC** | **is any of** and type the bcc address into the value field.
4 Click **Search** or **Save as Rule**.

Find email by cc

Find email by searching for email addresses on the **cc:** line.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.
2 Open the **Source/Destination** category.
3 Select **Email CC** | **is any of** and enter the cc address in the value field.
4 Click **Search** or **Save as Rule**.

Find email by domain

Find email in discovered data by searching for domain names.

The capture engine parses email addresses into three tokens, making it possible to find each component separately.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Discover** category.

3 Select **Domain Name** | **contains any of** and enter one or more domain names in the value field.

4 Click **Search** or **Save as Rule**.

Find email by port

Find email by using searching for email types that are transported through well-known ports.

For example, SMTP mail usually uses port 25, while HTTP webmail uses port 80.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Port** | **is any of**.

   Use **is none of** or use **source** or **destination** options to exclude or focus results.

4 Enter a port number in the value field.

5 Click **Search** or **Save as Rule**.

Find email by protocol

Find email by searching for the protocols used to send it.

For example, use the SMTP protocol to find corporate email, or the HTTP_Webmail protocol to find personal webmail.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Click **?**.

4 Open the **Mail Protocols** category.

5 Select one or more email types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find email by sender or recipient

Find email sent or received by specific users by setting the **sender** or **recipient** condition on the **Email Address** menu, then entering an email address in the value field.

If you want to identify both senders and recipients, select **Email Address** | **is any of** from the **Source/Destination** category.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **Email Address** | **sender is any of** or **Email Address** | **recipient is any of**.

Use **sender is none of** or **recipient is none of** to exclude specific addresses.

Use **+** to add more address parameters if you want to identify multiple sources and destinations.

4 Enter one or more email address in the value field.

5 Click **Search** or **Save as Rule**.

Find email by subject

Find email about specific topics by searching for the text contained in subject lines.

Click **+** to add an email address parameter if you want to narrow the query to a specific sender or recipient.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Enter an email subject in one of two ways:

- On the **Basic Search** menu, type the subject, then click **Search**.
- On the **Advanced Search** page, open the **Source/Destination** category, select **Email Subject** | **contains any of** and type the subject, then click **Search**.

Find webmail by port

Find webmail by port by searching using well-known port 80 for web traffic in your query.

By default, a port search returns results in both directions, but in separate flows. A port search is especially useful when the direction of traffic is known, but for complete results, define both source and destination values.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Port** | **source is any of** and type `80` in the value field.

4 Select **Port** | **destination is any of** and type `80` in the value field.

5 Click **Search** or **Save as Rule**.

Find webmail by protocol

Find webmail by searching for communications that use port 80. Web traffic commonly uses port 80.

You can use **Basic Search** to find all traffic on a single port quickly, but such a search is likely to return too many results. Use **Advanced Search** to add parameters that will focus your query.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Protocol** | **is any of** and click **?**.

The **Protocols** pop-up menu appears.

4 Open the **Mail Protocols** category.

5 Select one or more webmail types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find chat sessions

Find chat sessions by searching for chat content types. You can retrieve sessions lasting up to four hours.

Content of encrypted chat sessions (for example, Skype and AOL Instant Messenger 6) cannot be captured, but the duration of the chat is reported.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type is any of** and click **?**.

The **Content Types** pop-up menu appears.

4 Select the **Chat** category.

5 Select the chat protocol.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Chat sessions are reported in chronological order.

Search based on file parameters

When the search engine captures files, each file attribute is stored as a separate token in the capture database. You can find files by using any of the attributes of a file, such as type, owner, size or signature, in your search.

Examples:

- From the **Basic Search** menu, select **File Name Pattern** to target specific file types in **Data in Motion**.
- From the **Advanced Search** menu, select **Repository Type** from the **Discover** menu to find files that were found in **Data at Rest** during a CIFS scan.

You cannot search **Data in Use** at network endpoints.

Tasks

- *Find files by signature* on page 295
  Find files by searching for signatures created by the `SHA-2` algorithm (the `SHA-256` cryptographic hash function). The `SHA-256` sum utility creates compact digital signatures that can be used to find all copies of a uniquely-identified file.
- *Find files by size* on page 296
  Find files by adding a file size parameter to a query.
- *Find files by type* on page 296
  Find files by searching for specific file types.
- *Find document types* on page 297
  Find documents by searching for document file types.
- *Find Microsoft or Apple documents* on page 297
  Find Microsoft or Apple documents by searching with office documentation content types. The classification engine sorts all network data into content types, allowing searches for engineering drawings, different types of source code, office documents, images, and countless other file types.
- *Find office documents* on page 298
  Find common office documents that might be compromised by searching with office documentation content types.
- *Find proprietary documents* on page 298
  Find proprietary documents that might be compromised by searching for proprietary documents by content type.
- *Find files with human imagery* on page 299
  Find files with human imagery by searching with the **Fleshtone** concept. This feature makes it easy to identify advertising or x-rated sites.
- *Find images using file types* on page 299
  Find images by searching for file types used by graphics.

Finding document properties in context

Capture of document properties in context makes it possible to retrieve document metadata. Values in properties fields can be extracted only when they are associated with other values, increasing the granularity of search results.

For example, using the name of an author as a keyword in a search or rule would successfully retrieve that name from any location in the capture database. But using that name with the Microsoft Word *Author* property retrieves only the keyword in the defined context.

Types of document properties

Three document property types can be used to extract content in context from the capture database — predefined metadata, metadata added by users, or property values only.

Table 17-3 Types of document properties

Property type	Definition
Predefined properties	Standard properties shared by most document types, such as *author*, *keywords*, *subject*, and *title*. PDF files only support predefined properties.
Custom properties	User-defined properties added to the document metadata, allowed by some applications such as Microsoft Word. A user-defined property can also reference a standard document property that is not on the predefined properties list, but cannot duplicate a property that is on the list. User-defined custom properties in Microsoft Office 2007 and 2010 files are not supported.
Any property	Allows definition of a property by value alone. This useful in cases where the keyword has been entered in the wrong property parameter, or when the property name is unknown. For example, adding the value *Secret* to the *Any* property parameter classifies all documents that have the word *Secret* in at least one property.

Partial matching of document properties

Document properties definitions might be made up of one or more pre-defined or custom properties. When property values are defined, users can opt to allow partial matches — but partial matching of document properties is supported only on endpoint devices.

If a partial match is indicated, matches related to the property value are reported when the definitions are used in rules.

For example, you are looking for documents where Joseph D. Smith is the author. Specifying either *Joseph*, *Mr. Smith*, or *J. D. Smith* will trigger a match.

Add document properties and groups

You can use document properties and groups of document properties to retrieve objects through their attributes, and narrow the search to the context in which they are used.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies** | **Document Properties**.
- On your McAfee DLP appliance, select **Policies** | **Document Properties**.

2 From the **Actions** menu of the **Document Properties** or **Document Properties Group**, select **Add**.

3 Enter a name and optional description.

4 Select the components of the property or property group.

- In the **Create Document Properties** window, select properties and add instances of those property values as needed.
- In the **Create Document Properties Group** window, select the properties that are to be included in the group.

5 Click **Save**.

Find files by signature

Find files by searching for signatures created by the `SHA-2` algorithm (the `SHA-256` cryptographic hash function). The `SHA-256` sum utility creates compact digital signatures that can be used to find all copies of a uniquely-identified file.

You cannot use file signatures in direct queries, but you can find matches by adding them as rule parameters.

The `SHA-256` sum utility is available only on the Model 4400 appliance, but for legacy appliances you can use open source file checksum tools to generate a unique signature.

Task

1 Log on to the back end of the McAfee DLP Manager or McAfee DLP Monitor appliance.

2 Go to the /usr/bin directory on the Model 4400 appliance and locate the `sha2sum` utility.

3 Type in the command line utility to generate a signature.

```
# sha256sum <filename>
```

4 Select and copy the resulting hexadecimal number.

5 Open a browser and launch the McAfee DLP user interface. Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

6 Click a policy to open it for editing, then click a rule.

7 On the **Edit Rule** page, open the **File Information** category.

8 Select **Signature** | **is any of** and paste the hexadecimal number in the value field.

9 Click **Save**.

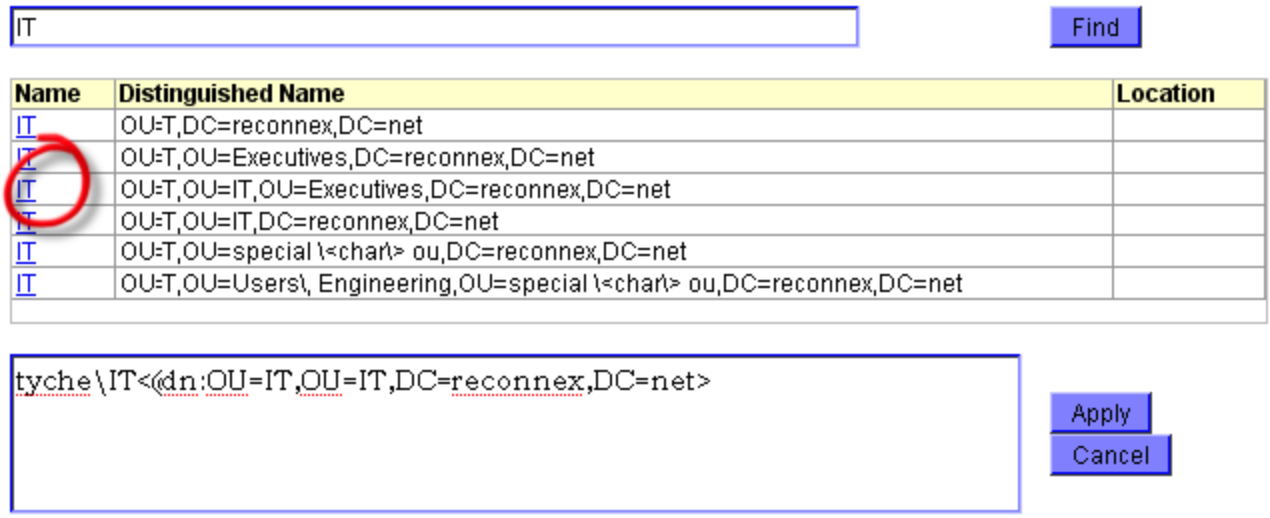
When the rule runs, the file will be detected and displayed on the McAfee DLP dashboards.

"Rule modification completed successfully" is displayed on the **Edit Policy** page.

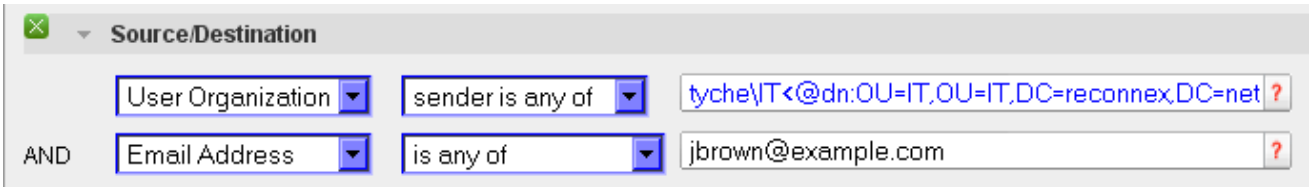
Find common names in different organizational units

Large enterprises sometimes have identical organizational names in multiple levels of the directory tree. When a query matches identical names in many different organizational units, you can locate the right one in the **Distinguished Name** column.

If you want to find a file name that is duplicated across organizational units in a directory server, you can determine the correct OU level by selecting it from the retrieved data.



For example, after selecting the right unit from the list, you might pair it with an email address to narrow the result to an individual in the unit.



Click **Search** or **Save as Rule** to complete the process.

Find files by size

Find files by adding a file size parameter to a query.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **File Information** category.

3 Select **File Size** | **range** and enter a value.

Select **greater than** or **less than** conditions to define upper or lower limits.

For example, 0-10 (less than 10 bytes), 100-1k (between 100 bytes and 1 kilobyte), 10M-1G (between 10 megabytes and 1 gigabyte).

4 Click **Search** or **Save as Rule**.

Find files by type

Find files by searching for specific file types.

Narrow your selection to one or two file types and add parameters to keep from getting too many results.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content type** | **is any of** and click **?**.

The **Content Types** pop-up menu appears.

4 Open a content type category and select checkboxes of file types.

5 Click **Apply**.

6 Click **Search** or **Save as Rule**.

Find document types

Find documents by searching for document file types.

Narrow your selection to one or two document types and add parameters to keep from getting too many results.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content type** | **is any of** and click **?**.

The **Content Type** pop-up menu appears.

4 Open the **Advanced Documents** category.

5 Select checkboxes of file types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find Microsoft or Apple documents

Find Microsoft or Apple documents by searching with office documentation content types. The classification engine sorts all network data into content types, allowing searches for engineering drawings, different types of source code, office documents, images, and countless other file types.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

The **Content Type** pop-up menu appears.

4 Open the **Microsoft** or **Apple Application** categories.

Microsoft Office documents are found in the **Office Documents** category.

5 Select checkboxes of file types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find office documents

Find common office documents that might be compromised by searching with office documentation content types.

Narrow your selection to one or two file document types to keep from getting too many results.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

The **Content Types** pop-up menu appears.

4 Open the **Office Applications** category.

5 Select checkboxes to define one or more office document types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find proprietary documents

Find proprietary documents that might be compromised by searching for proprietary documents by content type.

Narrow your selection to one or two file document types to keep from getting too many results.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

The **Content Types** pop-up menu appears.

4 Open the **Engineering Drawings and Designs** category.

5 Select checkboxes to define one or more design document types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find files with human imagery

Find files with human imagery by searching with the **Fleshtone** concept. This feature makes it easy to identify advertising or x-rated sites.

Add a **Thumbnail Match** column to your dashboard to scan results quickly. Avoid timeouts caused by retrieving large image files by adding additional search terms.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Concept** | **is any of** and enter `Fleshtone` in the value field.

4 Click **Search** or **Save as Rule**.

Find images using file types

Find images by searching for file types used by graphics.

Add a **Thumbnail Match** column to your dashboard to scan results quickly. Avoid timeouts caused by retrieving large image files by adding additional search terms.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content type** | **is any of** and click **?**.

The **Content Types** pop-up menu appears.

4 Open the **Image** category.

5 Select checkboxes of image file types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Search discovered data

Sensitive data that has been discovered in network repositories is stored in the McAfee DLP Discover database, and is searchable through McAfee DLP Manager.

The **Advanced Search** and **Edit Rule** pages list a **Discover** category that includes a list of options for searching discovered data.

Those parameters can be used alone or in combination with other attributes to retrieve narrow ranges of discovered data.

Find registered files in data at rest

Find registered files in discovered data by using the **DocReg** concept with one of the **Discover** parameters.

Use **Share Name** or **File Path** to define a location at which you want to find registered data.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Share Name** or **File Path**.

3 Type the share name or file path into the value field.

4 Click **Search**.

Find scan operations in data at rest

Find scan operations in discovered data by using the **Scan Operation** attribute in a query.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, accept the default **Scan Operations**.

3 Click **Search**.

Find host IP addresses in data at rest

Find a host IP address in data at rest by using the **Host IP** attribute in a query.

Indicate a choice between two IP addresses by separating them with a comma (no spaces). You can search for single IP addresses, ranges, subnets, and addresses expressed in CIDR notation (see examples below).

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Find a host IP address in **Data-at-Rest** in one of two ways:

- On the **Basic Search** page, select **Host IP**, and type one or more host IP addresses.
- On the **Advanced Search** page, open the **Discover** category, select **Host IP**, and type one or more host IP addresses.

3 Click **Search**.

Examples

192.168.3.225

10.0.1.255–10.1.0.10

172.16.1.1/24

Find host names in data at rest

Find a host name in data at rest by using the **Host Name** attribute in a query.

Indicate a choice between two host names by separating them with a comma (no spaces).

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Find a host name in **Data-at-Rest** in one of two ways:
- On the **Basic Search** page, select **Host name**, and type one or more host names.
- On the **Advanced Search** page, open the **Discover** category, and type one or more host names.

3 Click **Search**.

Find domain names in data at rest

Find domain names in discovered data by using the **Domain Name** attribute in a query.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Domain Name**.

3 Click **Search**.

Find share names in data at rest

Find share names in discovered data by using the **Share Name** attribute in a query.

On Microsoft Windows computers, the default share is `C$`.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Share Name**.

3 Click **Search**.

Find file name patterns in data at rest

Find file name patterns in discovered data by using the **File Name Patterns** attribute in a query.

You can also use this attribute in a **Basic Search** to find files in network data.

The only metacharacter supported is a single asterisk. Comma- and space-separated values signifying AND and OR are not supported.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **File Name Pattern contains any of**.

   You can use a keyword with an asterisk (for example, Financ*), but a **File Name Pattern** search is faster.

3 Type a name or file type extension into the value field.

4 Click **Search**.

Find repository types in data at rest

Find repository types in discovered data by using the **Repository Type** attribute in a query.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Repository Type**.

3 Click **Search**.

Find file paths in data at rest

Find file paths in discovered data by using the **File Path** attribute in a query.

Absolute or relative file paths in Microsoft Windows (\) or UNIX (/) systems are indexed in the database, but only UNIX paths are supported when searching.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **File Path is any of**.

3 Type the file path into the value field.

4 Click **Search**.

Find file owners in data at rest

Find file owners in data at rest by using the **File Owner** attribute in a query.

Indicate a choice between two file owners by separating them with a comma (no spaces).

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 Find a file owner in **Data-at-Rest** in one of two ways:
- On the **Basic Search** page, select **File Owner**, and type one or more user names.
- On the **Advanced Search** page, open the **Discover** category, select **File Owner**, and type one or more user names.

3 Click **Search**.

Find catalogs in data at rest

Find catalogs in discovered data by using the **Catalog** attribute in a query.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Catalog**.

3 Click **Search**.

Find schema names in data at rest

Find schema names in discovered data by using the **Schema Name** attribute in a query.

Database design varies by vendor, but all vendors use schemas.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Schemas**.

3 Click **Search**.

Find table names in data at rest

Find table names in discovered data by using the **Table Name** attribute in a query.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Table Name**.

3 Click **Search**.

Find column names in data at rest

Find column names in discovered data by using the **Column Name** attribute in a query.

Database design varies by vendor, but all vendors use columns.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Column Name**.

3 Click **Search**.

Find records and rows in data at rest

Find records and rows in discovered data by using the **Records and Rows** attribute in a query.

Database design varies by vendor, but all vendors use records and rows.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Records and rows**.

3 Click **Search**.

Find signature percentage matches in data at rest

When registered text is plagiarized, it is unlikely that a 100 percent match will be found to the original document. Finding only a percentage of the registered material is more likely to expose intellectual property theft.

The **Signature Percentage Match** parameter can only be added to a rule to supplement other parameters that have been defined. It is not possible to find percentage matches of registered data in a search.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Policies**.
- On your McAfee DLP appliance, select **Policies**.

2 Open a policy, or add a new one.

3 From the **Actions** menu, select **Add Rule**.

4 Open the **Content** category.

5 From the drop-down lists, select **Concept is any of** and click **?**.

The **Concepts** pop-up menu appears.

6 From the **Corporate Confidential** category, select **DocReg**.

The **DocReg** concept contains all of the signatures that were added during document registration.

7 From the **Discover** menu, select **Signature Percentage Match**.

Because an exact percentage match is unlikely, the match can only be greater than the percentage you specify.

8 Enter an integer in the value field.

9 Click **Save**.

When the rule is run, the **DocReg** signatures are matched against data in network file systems, and results are reported on the **Data-at-Rest** dashboard.

Search with the DocReg concept

Searching with the **DocReg** concept applies all existing signatures to the network data stream, network repositories, and endpoints.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Content** menu, select **Concept is any of**.

3 Type **DocReg** into the value field.

4 Click **Search**.

Typical scenarios

To find significant data in network traffic, use search parameters to form queries. Some typical use cases follow.

Tasks

- *Find leaked documents* on page 306
  Whether accidental or unintentional, confidential documents on corporate networks are often open to discovery by unauthorized users.
- *Monitor sensitive files after close of business in different time zones* on page 307
  If you are managing several McAfee DLP Monitor appliances in different time zones, you might want to monitor data at the same local clock time in every location. For example, certain files might be allowed to enter or leave local networks during business hours — but after 5 p.m. in any time zone, it might indicate a leak.
- *Find email using non-standard ports* on page 307
  When non-standard ports are used to transmit email, a deliberate attempt to conceal illegal activity should be suspected.
- *Find evidence of frequent communications* on page 308
  You might suspect that a particular user is communicating with an off-site competitor. You might be able to identify the sources and destinations of frequent communications that will eventually reveal that leak.
- *Find source code leaving the network* on page 309
  You can use the **Source Code** content type to find intellectual property that might be leaving the company.
- *Find encrypted traffic and files* on page 309
  Insiders attempting to conceal illegal activity or steal your intellectual property routinely use encryption.
- *Find unencrypted user data* on page 310
  You might assume that user names and passwords are protected on your network as a matter of course, but that might not always be the case.
- *Find geographic users and incidents* on page 310
  The classification engine sorts all network data into geographic locations. Find incidents generated by users in other countries by defining geographic locations in your query.
- *Find evidence of foreign interference* on page 310
  Protecting intellectual property can be difficult when sensitive data is so easily transported beyond national borders.
- *Search for social networking activity* on page 311
  Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.
- *Find postings to message boards* on page 311
  Employees sometimes spend company time posting to Internet sites that are not work-related.
- *Find frequently visited web sites* on page 312
  Find web sites that are frequently visited by users who might routinely use the Internet to complete their job duties, but might enter URLs that can compromise network security.

Find leaked documents

Whether accidental or unintentional, confidential documents on corporate networks are often open to discovery by unauthorized users.

This case helps you to locate leaked documents, then analyze the incidents to find out how they were leaked.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Basic Search**.
- On your McAfee DLP appliance, select **Capture** | **Basic Search**.

2 Select **Input Type** | **Keywords**, then type a word or phrase that might be found in a sensitive document, such as `Confidential`.

If you have additional information (such as content type or protocol), use an **Advanced Search** so you can add elements to include those values.

3 Select a time frame from the **Date/Time** menu.

4 Click **Search**.

Monitor sensitive files after close of business in different time zones

If you are managing several McAfee DLP Monitor appliances in different time zones, you might want to monitor data at the same local clock time in every location. For example, certain files might be allowed to enter or leave local networks during business hours — but after 5 p.m. in any time zone, it might indicate a leak.

The date and time set on your DLP appliances is determined by the local time zone in which they were installed. Because local time is automatically converted to Greenwich Mean Time (GMT), you must use the **Exact Time** parameter and set a **local time** condition.

By creating a rule that tracks sensitive data between the hours of 5 and 6 p.m. in your Los Angeles, New York, London, and Tokyo offices, you can monitor data at the time most employees are leaving each of those facilities.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Date/Time** category and select **Exact Time**.

3 From the conditions menu, select **before**, **between**, or **after (local time)**.

Select **between (local time)** to set both **before** and **after** delimiters.

4 From the calendar icon, select a date, and set hour, minute and second times with the thumbwheel menus.

5 Click **Search** or **Save as Rule**.

Find email using non-standard ports

When non-standard ports are used to transmit email, a deliberate attempt to conceal illegal activity should be suspected.

This case helps you to eliminate email that uses well-known ports, so that unknown or unsecured transmissions can be revealed.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

4 From the **Mail** menu, select one or more email formats.

5 Click **Apply**.

6 Open the **Protocol** category.

7 Select **Port** | **is none of** and type one or more standard email port numbers into the value field.

Ports 25 and 80 are commonly-used email and webmail ports.

8 Click **Search**.

Port information is displayed in the **Source** and **Destination** columns; add them to the dashboard if necessary.

Find evidence of frequent communications

You might suspect that a particular user is communicating with an off-site competitor. You might be able to identify the sources and destinations of frequent communications that will eventually reveal that leak.

This case helps you to find the other side of a session by searching for a **UserID** or email address.

If the source and destination IP addresses are dynamically assigned, they will change over time. If you have added a DHCP server to McAfee DLP Manager, you can track the previous addresses of a host. Add another parameter to identify both sides of a conversation to find both sources and destinations of communications.

Task

1 Select one of these options:
- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 Select an incident.

3 From the **Filter by** | **Timestamp** menu, select a time frame.

4 Click the plus icon to add another parameter, then select **SourceIP** | **equals**.

5 Enter an IP address that you retrieved from the incident.

6 Click **Apply**.

7 Examine the incidents on your dashboard to find the **DestinationIP** that matches up to the **SourceIP**.

Find source code leaving the network

You can use the **Source Code** content type to find intellectual property that might be leaving the company.

Narrow your selection to one or two source code types to keep from getting too many results.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

   The **Content Types** pop-up windows appears.

4 Open the **Source Code** category, then select checkboxes to define one or more code types.

5 Open the **UNIX** category, then select checkboxes to define one or more shell scripts.

6 Click **Apply**.

7 Click **Search**.

Find encrypted traffic and files

Insiders attempting to conceal illegal activity or steal your intellectual property routinely use encryption.

This case helps you to identify the sources and destinations of encrypted traffic and files on your network to expose those activities.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
   - On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

4 From the **Binary** menu, select **Binary**.

5 From the **Office Applications** menu, select **EncryptedPowerpoint**, **EncryptedExcel**, **EncryptedWord**, **EncryptedPDF** and **PDF**.

6 From the **Protocol** menu, select **Crypto**.

7 Click **Apply**.

8 Click **Search**.

Find unencrypted user data

You might assume that user names and passwords are protected on your network as a matter of course, but that might not always be the case.

This case helps you to find out quickly if user account information is circulating in clear text on your network by searching for account passwords.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Basic Search**.
- On your McAfee DLP appliance, select **Capture** | **Basic Search**.

2 Select **Input Type** | **Keywords**, and type the words `account password` into the value field.

3 Click **Search**.

If there are any significant results, alert your IT department.

Find geographic users and incidents

The classification engine sorts all network data into geographic locations. Find incidents generated by users in other countries by defining geographic locations in your query.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **GeoIP location** | **is any of** and click **?**. Use **is none of** to exclude a geographic location.

The **GeoIP Locations** window appears.

4 Select continents and/or countries from the lists.

5 Add **Sender** and **Recipient** values to find users in the defined geographic locations.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find evidence of foreign interference

Protecting intellectual property can be difficult when sensitive data is so easily transported beyond national borders.

This case helps you to identify source and destination IP addresses that will tell where suspicious traffic is coming from and where it is going.

Because dynamically assigned IP addresses change regularly, hosts that are not local can be identified only if a DHCP server is installed on the network.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Basic Search**.
- On your McAfee DLP appliance, select **Capture** | **Basic Search**.

2 Select **Input Type** | **GeoIP Location** and click **?**.

3 Select one or more country names from the pop-up menu.

4 Click **Apply**, then **Search** and examine the incidents on your dashboard.

If you do not see locations in your results, click **Columns** and add **Source**, **Destination**, **Sender** or **Recipient** columns to the dashboard.

Search for social networking activity

Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.

This case helps you to find out how much social networking activity is occurring on your network by identifying all traffic to and from specific web sites.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting**.
- On your McAfee DLP appliance, select **Capture**.

2 On the **Basic Search** page, select an **Input Type** and click **?**.

- Select **Protocols**, then HTTP_Post from an **Internet Protocols** menu. Click **Apply**, then **Search**.
- Select **Keywords**, type keywords (for example, `facebook` or `deadspin`), then **Search**.

Find postings to message boards

Employees sometimes spend company time posting to Internet sites that are not work-related.

This case helps you to identify that activity by targeting the protocol that is used to transmit such postings.

This filter identifies all posting traffic. If you know what web site it is being posted to, add a **Content** | **equals** parameter and type its name (for example, `webrats.com`).

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

2 From the **Filter by** menu, select a time from the **Timestamp** sub-menu.

3 Click the plus icon to add a filter and select **Protocol** | **equals**.

4 Click **?**, select a protocol from the pop-up list, then click **Apply**.

5 Click **Apply**.

Find frequently visited web sites

Find web sites that are frequently visited by users who might routinely use the Internet to complete their job duties, but might enter URLs that can compromise network security.

This case creates a content capture filter to store all traffic to and from inappropriate web sites to find out if your company policy is being violated.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Advanced Search**.
- On your McAfee DLP appliance, select **Capture** | **Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **URL** | **is any of** and type the URL of the website into the value field.

For example, type in `www.deadspin.com`.

4 Click **Search**.

If no results are retrieved, check to see if the default `ignore_http_header` content capture filter is still active.

18 Capture filters

Capture filters are used to filter out large portions of data and network traffic that do not require analysis by the capture engine.

Contents

- *How capture filters work*
- *Manage capture filters*
- *Typical scenarios*

How capture filters work

Filtering network data can cut down on the vast amounts of data captured and analyzed, so it is important to tune the system using capture filters when it is set up.

When deployed, capture filters constrain the network data stream by recognizing only the most significant data for investigation, and as a result, performance is enhanced.

You can also use capture filters to store critical sessions and applications-level data.

When the capture engine captures and indexes all TCP/IP traffic, it is broken down into content types. Anything that cannot be identified is tagged *Unknown*.

Types of capture filters

Capture filter types are determined by the layer of the OSI (Open Systems Interconnection) model that is recognized and stored by the capture database.

There are two capture filter types.

- **Content capture filters** filter out specific content types, eliminating significant portions of Application layer data
- **Network capture filters** filter out or store network traffic on the Transport Layer, usually in a specific sequence.

Content capture filters are used to streamline data capture and improve performance. Network capture filters can be used to do more complex tasks, like finding spiders, robots, crawlers, types of webmail, browser versions, and operating systems in use.

Types of capture filter actions

Capture filter actions exclude or store large amounts of captured data. The actions available differ, depending on whether the filter is designed to work on the Application or Transport layer.

There are two capture filter action types, and several sub-types that extend the functionality of content and network capture filters.

Content capture filters allow administrators to configure the capture engine to drop elements, sessions or store element only metadata.

For example, if your network has a large cache of video files that you know are not a security threat because you have controlled them with configuration management software, you can set up a filter that drops those elements, saving time and resources for analysis of data at risk. Similarly, if your employees are authorized to send or receive any SMTP content that is processed by your company's mail server, you can drop those communications.

Network capture filters allow administrators to configure the capture engine to ignore or store traffic types.

For example, if you want to know what kind of data is moving through the network data stream without storing its content, storing metadata allows you to keep incidental information (like the source and destination of the data, data types being transmitted, and protocols being used to transmit it).

Types of content capture filter actions

Content capture filter actions drop elements or sessions from network traffic, or store only metadata.

There are three types of content capture filter action.

- **Drop element** keeps a particular type of content from being captured. For example, if your network has a large cache of video files that you know are not a security threat because you have controlled them with configuration management software, you can set up a filter that drops these secure files, saving time and resources for analysis of data at risk.
- **Drop Sessions** filters out sessions containing the defined elements from being captured. For example, if your employees are authorized to send or receive any SMTP content that is processed by your company's mail server, you can drop those communications.
- **Drop element; store metadata only** keeps all content from being captured, but retains all of the attributes that define the objects captured and stored in the database. For example, if you want to know what kind of data is moving through the network data stream without storing its content, storing metadata allows you to keep incidental information (like the source and destination of the data, data types being transmitted, and protocols being used to transmit it).

Types of network capture filter actions

Network capture filter actions ignore or store network data, depending on port or protocol used.

There are two types of network capture filter action.

- **Ignore** keeps a particular type of traffic from being captured. For example, you can ignore all web traffic by using HTTP filters, or eliminate authorized email by ignoring traffic using port 25 (SMTP).
- **Store** stores a particular type of network traffic. For example, you can store chat traffic by creating a filter that identifies and keeps data transmitted using AOL_Chat, MSN_Chat, or Yahoo_Chat protocols.

How content capture filters work

Content capture filters filter out or store specified types of data that are transmitted on the Application layer (also known as Flow A).

Standard content capture filters perform routine operations on network data to improve McAfee DLP performance and results.

Table 18-1 Standard content capture filters

Content capture filter	Purpose
Ignore binary	Exclude binary files from network traffic
Ignore BMP and GIF images	Exclude BMP and GIF images from network traffic

Table 18-1 Standard content capture filters *(continued)*

Content capture filter	Purpose
Ignore crypto	Exclude encrypted data from network traffic
Ignore HTTP GZip responses	Keep compressed files from being opened by the capture engine
Ignore HTTP headers	Keep HTTP header blocks from being captured
Ignore P2P	Keep Peer-to-Peer traffic from being captured
Ignore small JPG images	Excludes insignificant images (smaller than 4 MB) from network traffic
Ignore flow headers	Keeps flow headers from being recognized

How network capture filters work

Network capture filters included with McAfee DLP systems filter data streaming on the Transport Layer to improve performance and isolate significant traffic.

Network capture filters work by eliminating large portions of Transport (Layer 4) traffic. They operate in a cumulative sequence and always terminate in the BASE filter, which stores the configuration.

For example, most businesses are interested in monitoring traffic carried to or from external IP addresses. When the RFC (Request for Comments) 1918 filter is active, IP addresses set aside by IANA (Internet Assigned Numbers Authority) for internal use can be excluded from analysis by the capture engine.

Table 18-2 Standard network capture filters

Network capture filter	Purpose
Ignore RFC 1918	Excludes traffic routed to 10.0.0.0.-10.255.255.255, 172.16.0.0.-172.31.255.255 and 192.168.0.0-192.168.255.255
Ignore HTTP Responses	Excludes program output sent from a server after receiving and interpreting an HTTP Request
Ignore unknown	Excludes traffic using unknown protocols
Ignore SMB	Excludes Session Message Block and Microsoft Basic Input/Output System (NetBIOS) traffic
Ignore SSH	Excludes Secure Shell traffic
Ignore POP	Excludes Post Office Protocol 3 traffic
Ignore IMAP	Excludes Internet Message Access Protocol traffic
Ignore HTTPS	Excludes secure Hypertext Transport Protocol traffic
Ignore LDAP	Excludes Lightweight Directory Access Protocol traffic
Ignore NTLM	Excludes Microsoft New Technology Local Area Network Manager traffic
BASE	Base Configuration filter (opens the system for storage of incoming data)

Manage capture filters

Create, deploy and manage capture filters.

Tasks

- *Add content capture filters* on page 316
  Add content capture filters to identify types of Application Layer traffic that can be stored or ignored. After these blocks of data are identified, the capture engine will not capture or parse any of the traffic containing them.
- *Add network capture filters* on page 317
  Add network capture filters to identify types of Transport Layer traffic that can be stored or ignored. After these blocks of data are identified, the capture engine will not capture or parse any of that traffic.
- *Copy capture filters* on page 318
  If you have two or more McAfee DLP appliances of the same type registered to McAfee DLP Manager, you can copy the capture filter configuration to another device.
- *Deploy capture filters* on page 318
  Deploy capture filters on McAfee DLP Monitor devices so that they can be applied to the network data stream. If undeployed, the **None** box will be checked, and the filter will be saved but not run.
- *View deployed capture filters* on page 318
  View capture filters on the **System** dashboard to find out which ones are deployed on McAfee DLP Manager or a McAfee DLP Monitor.
- *Remove deployed capture filters* on page 319
  Remove deployed capture filters to break their links to specific McAfee DLP devices.
- *Reprioritize capture filters* on page 319
  Reprioritize network capture filters to define specific positions on the list of filters. This is necessary because the order in which network capture filters are deployed has a cumulative affect on captured traffic.
- *Modify capture filters* on page 320
  Modify capture filters by editing their parameters.

Add content capture filters

Add content capture filters to identify types of Application Layer traffic that can be stored or ignored. After these blocks of data are identified, the capture engine will not capture or parse any of the traffic containing them.

Before you begin
Make a note of the types of Flow A traffic you want the capture engine to store or ignore.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 Click **Create Content Filter**.

3 Type in a filter name and optional description.

4 Select the devices to which the capture filter is to be deployed.

If you want to deploy a capture filter at a later time, select **None**.

5 Select a capture action to indicate what portion of traffic is to be stored or dropped.

6 Open each category and define parameters that describe the traffic.

7 Click **Save**.

The **Capture Filters** page reappears.

8 Test the filter with live traffic and modify it until it is working correctly.

Add network capture filters

Add network capture filters to identify types of Transport Layer traffic that can be stored or ignored. After these blocks of data are identified, the capture engine will not capture or parse any of that traffic.

On the **Network Filter** page, open **All**. This action either captures or cuts off all traffic, depending on the capture action you select, so that you can observe a limited pool of data before deciding what to filter.

Designing network capture filters require experimentation because the order in which they are deployed is crucial, but taking the time to streamline the capture process can save a lot of processing time. When a network capture filter is applied to the network data stream, its position in the list indicates its priority. Because the BASE filter instructs the system to store all data that has not been dropped from the data stream, it must always run last.

Task

1 Make a note of the types of traffic you want the capture engine to store or ignore.

2 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

3 Click **Create Network Filter**.

4 Type in a filter name and optional description.

5 Select a capture action to indicate what portion of traffic is to be stored or dropped.

6 Select the devices to which the capture filter is to be deployed.

If you want to deploy a capture filter at a later time, select **None**.

7 Open each category and define parameters that describe the traffic that is to be stored or dropped.

8 Click **Save**.

The **Capture Filters** page reappears.

9 In the **Network Filters** table, use the **Priority** arrows to move the filter into the correct position.

When establishing a sequence for applying network capture filters to the network data stream, remember that changing the order of a single filter might skew your results.

10 Test the filter with live traffic and modify it until it is working correctly.

Copy capture filters

If you have two or more McAfee DLP appliances of the same type registered to McAfee DLP Manager, you can copy the capture filter configuration to another device.

Before you begin

Configure capture filters on one of the McAfee DLP appliances you plan to copy.

For example, you might copy capture filters from one McAfee DLP Discover to another, or from one McAfee DLP Monitor to another.

Both appliances must be registered to the same McAfee DLP Manager.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 On the **Capture Filter** page, scroll down to locate the device to which you are copying the configuration.

3 Click the **Add Filter** pop-up and select a device.

If the list is empty, you cannot copy the filter.

4 Click **Apply**.

The device information in the capture filter is updated.

Deploy capture filters

Deploy capture filters on McAfee DLP Monitor devices so that they can be applied to the network data stream. If undeployed, the **None** box will be checked, and the filter will be saved but not run.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 From the list of capture filters, select one that is undeployed.

The default display shows filters by device. To view undeployed filters, change the **Views** to display either all content filters or all network filters.

3 From the **Devices** box, check the device on which you want to install the capture filter.

4 Click **Save**.

View deployed capture filters

View capture filters on the **System** dashboard to find out which ones are deployed on McAfee DLP Manager or a McAfee DLP Monitor.

If you are using a standalone McAfee DLP Monitor, you will see only the filters deployed on your own machine.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 On the list of capture filters, note the name of the system before each group of capture filters.

Scroll down the page if McAfee DLP Manager is managing more than one McAfee DLP Monitor.

Remove deployed capture filters

Remove deployed capture filters to break their links to specific McAfee DLP devices.

Deploying capture filters at the time they are created is optional.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 Open a capture filter deployed to a device.

3 Select the **None** checkbox under **Devices**.

4 Click **Save**.

Reprioritize capture filters

Reprioritize network capture filters to define specific positions on the list of filters. This is necessary because the order in which network capture filters are deployed has a cumulative affect on captured traffic.

Content capture filters do not require priority; they can be listed in any order.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 On the list of network capture filters by device, click up and down arrows until the proper order is established.

Because the BASE filter instructs the system to store all data that has not been dropped from the data stream, it must always run last.

3 Click **Apply**.

Modify capture filters

Modify capture filters by editing their parameters.

The system might take some time to reflect modifications because this affects the action of the capture engine while it is in operation.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 From the list of capture filters, click the one that you want to modify.

To view undeployed capture filters, change the **Views**.

3 On the **Filter** page, edit the parameters of the filter to be modified.

4 Click **Save**.

Typical scenarios

Use the following use cases to get a general understanding of how capture filters can be used to control the data recognized by the capture engine.

Tasks

- *Filter out traffic using common IP addresses* on page 320
  Filter out portions of traffic using one or more IP addresses that comprise a large portion of your network traffic. Drop or store that data to reveal more significant traffic.
- *Manage data capture with network capture filters* on page 321
  Manage data capture using multiple capture filters that instruct the capture engine to ignore successive levels of traffic, while making an exception for a subset of traffic within a defined flow. You can use port numbers to filter specific types of traffic.
- *Exempt users from detection* on page 322
  Even network administrators might not be privileged to peruse certain information found in network data streams.

Filter out traffic using common IP addresses

Filter out portions of traffic using one or more IP addresses that comprise a large portion of your network traffic. Drop or store that data to reveal more significant traffic.

For example, you might drop specific IP addresses that are well-known within your intranet, a range of addresses, or all addresses on a subnet. These addresses, also known as elements, will be removed from consideration by the capture engine. In addition, you might expand drop all of the sessions containing those elements, or you might opt to store only the metadata defining them.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 Click **Create Content Filter**.

3 Enter a **Filter Name** and optional **Filter Description**.

4 Select the devices on which the capture filter is to be deployed.

5 Select a capture filter action.

For example, you might drop all traffic containing the addresses from the Application or Transport layers, or you might store only the metadata defining the addresses.

6 Open the **Source/Destination** category.

7 Select **IP Address** and add a condition.

For example, you might define all of the IP addresses, all but the defined addresses, or addresses moving in one direction only.

8 Type one or more IP addresses in the value field.

9 Click **Save**.

Manage data capture with network capture filters

Manage data capture using multiple capture filters that instruct the capture engine to ignore successive levels of traffic, while making an exception for a subset of traffic within a defined flow. You can use port numbers to filter specific types of traffic.

The order in which you deploy capture filters is significant, so planning the process is essential.

For example, if you want McAfee DLP Manager to ignore encrypted data, it could easily be done by eliminating traffic transported through port 443 on McAfee DLP Monitor. But if you have to capture AIM (AOL Instant Messaging) traffic to monitor chat, you must add an exception, because AOL also uses port 443.

You cannot save sessions or data that have already been eliminated, so the filtering sequence is crucial.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

2 Click **Create Network Filter**.

3 Type a filter name (for example, `AOL_Chat`) and an optional description.

4 From the **Action** menu, select **Store** to capture AOL chat traffic.

5 Open the **Protocol** category.

6 Select **Protocol** | **is any of** and click **?**.

7 From the **Protocol** pop-up menu, select **Chat Protocols** | **AOL_Chat** and **Apply**.

8 Click **Save** to complete the AOL chat filter.

9 Click **Create Network Filter** to create another filter.

10 Type a filter name (for example, `SSH_traffic`) and an optional description.

11 From the **Action** menu, select **Ignore**.

12 Open the **Protocol** category and select **Port** | **source is any of**, then type `443` into the value field.

This stores incoming encrypted data. Traffic through ports and port ranges is bidirectional, so you must define source and destination transmissions separately. You will have capture both sides of excluded transmission to capture both sides of the chat within it.

13 Click **+** to add a parameter.

14 Repeat the process, but select **Port** | **destination is any of** and type `443` into the value field.

This stores outgoing encrypted data.

15 Select the checkbox of the device on which you want the filter deployed.

To decide later, click **None**.

16 Click **Save**.

A new **Ignore** filter, which excludes encrypted data from processing by the capture engine, is added to the existing capture filter list.

17 In the **Network Filters** list, use the **Priority** icons to reorder the filters.

When a network capture filter is applied to the network data stream, its position in the list indicates its priority. Because the BASE filter instructs the system to store all data that has not been dropped from the data stream, it must always run last.

The `AOL_chat` **Store** filter must run first, because the `SSH_traffic` **Ignore** filter will eliminate what remains of the port 443 traffic.

18 Let the system run. After some time, you can search for AIM chats in the captured data on the **Incidents** page.

Exempt users from detection

Even network administrators might not be privileged to peruse certain information found in network data streams.

Before you begin

Endpoint features require deployment of McAfee DLP Endpoint and an added evidence server.

This case helps you to ensure absolute security for one or more endpoints that have access to top secret information by protecting them from detection by the capture engine.

Alternately, use this procedure with a user or group name, or an email address.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration**.
- On your McAfee DLP appliance, select **System** | **System Administration**.

2 Select **Capture Filters** from the left pane options.

Filters are displayed by device in the right panel.

3 Click **Create Content Filter**.

4 Type a filter name and optional description.

5 Select **Action** | **Drop Element**.

6 Open the **Source/Destination** category.

7 Select **IP Address** | **is any of** and type an IP address into the value field.

If the address is on a subnet, it is detectable only if the network and host portions of an IP address are standard classful IP (address fields are separated into four 8-bit groups). Separate multiple addresses by commas, and IP ranges by dashes.

8 Select the checkbox of the device on which you want the filter deployed.

To decide later, click **None**.

9 Click **Save**.

A new capture filter is added to the existing list.

Maintenance

Chapter 19 *Managing McAfee DLP systems*
Chapter 20 *Disaster recovery backup and restore*
Chapter 21 *Technical support*

19 Managing McAfee DLP systems

Performing general maintenance tasks helps your McAfee DLP appliances to operate as intended.

Contents

- *Configure McAfee DLP system information*
- *Add McAfee DLP devices to McAfee DLP Manager*
- *Unregister McAfee DLP devices*
- *Restart McAfee DLP appliances or services*
- *Change link speed*
- *Manage McAfee DLP appliance disk space*
- *Monitoring audit logs*
- *SNMP management*
- *Using network statistics*
- *Technical specifications*

Configure McAfee DLP system information

Configure McAfee DLP devices during installation by running the **Setup Wizard**, or after installation by making changes on the **System Configuration** page of the device.

With this release, the **Devices** page is refreshed automatically every two minutes to reflect the new status of the devices and statistics.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 Select a device and click **Configure**.

3 Change parameters on the **System Configuration** page.

4 Click **Update** after each change is made.

Server locale is not configurable by users.

Add McAfee DLP devices to McAfee DLP Manager

Adding a device to McAfee DLP Manager will remove the current policy, configuration, incidents, and cases on the device.

Before you begin

If you are using the default root password on a McAfee DLP device, log on to the command line interface of the McAfee DLP device to change the password before adding the device to McAfee DLP Manager.

If there is any existing configuration or data on the device, McAfee recommends reinstalling the appliance before adding it to McAfee DLP Manager.

Devices added to McAfee DLP Manager will be assigned any policies that are configured for **All Devices**. If **All Devices** is not selected in a policy, the policy must be manually configured to include the new device after the device is added.

A managed device can be converted to a standalone state by reinstalling the device.

You cannot add McAfee DLP Endpoint to McAfee DLP Manager using this procedure.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP Manager appliance, select **System** | **System Administration** | **Devices**.

2 Select **Actions** | **New Device**.

3 Enter the device IP address or host name and the root password.

4 Click **Add**.

5 Click **OK** to confirm or **Cancel** to cancel the registration.

6 To check the status, refresh the page.

When the **Status** icon in the device list to turns green, registration is complete.

Unregister McAfee DLP devices

Unregister McAfee DLP devices if you have to re-synchronize a timed-out system, overwrite an older configuration, or register a device to a different McAfee DLP Manager.

If you will reconfigure the device as a standalone system, you must reinstall it.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 In the **Advanced** column, click **More** for a specific device.

3 Scroll down to **Restart/Shutdown** and select **Deregister device**.

4 Click **OK** or **Cancel**.

Because the messaging service must be restarted whenever a device is unregistered, you might get a logon error message like "could not connect to service" before you can log on again. If so, the messaging service will generally be back up in 1-3 minutes.

5 Confirm that the unregistered device has been removed from the list on the **Devices** page.

Restart McAfee DLP appliances or services

Restart, shut down or reboot McAfee DLP appliances to clear problems.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 In the **Advanced** column, click **More** for a specific device.

3 Scroll down to **Restart/Shutdown**.

4 Click either the **Restart console server**, **Reboot device**, or **Power-down device** command.

Change link speed

Change link speed if devices installed on the network have specific speed and duplexing requirements. McAfee DLP Monitor might not be able to auto-negotiate traffic to capture interfaces.

Depending on your network configuration, you might have to replace your standard Ethernet cable with one that is appropriate for your network.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 Select a device from the list.

3 Click **Configure**.

4 In the **Capture Interfaces** section, select link speeds for each capture interface from the **Speed and Duplex** menus.

5 Click **Update**.

A notification message appears to verify the change.

Manage McAfee DLP appliance disk space

McAfee DLP appliance disk space varies from 0.5 to 10TB, depending on whether legacy or Intel appliances are used, and the configuration of each device. You can determine disk space by retrieving disk usage information on the appliances registered to McAfee DLP Manager.

The Reconnex file system (RFS) divides the McAfee DLP Monitor disk into partitions. Capture partitions hold all the content captured, which is organized by type. Non-capture partitions contain the operating system and the results partitions (A-Z), which fill sequentially.

The capacity of the capture partitions in the Intel Server System SR2612SR is 7.2TB (across 12 disks).

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 In the **Advanced** column, click **More** for a specific device.

3 Scroll down to **Application Information**.

4 Click **Disk usage**.

The `show_rfs_df` command runs, and the results are displayed on the page that opens.

Setting wiping policies

Wiping policies set the standard for usage of disk space on the McAfee DLP appliances. You can wipe captured data depending on how much space is used, or at fixed time intervals.

Wiping policies are set on the **System Configuration** page, which is accessible from the **Configure** link of each registered device.

Wiping policy types

Space-based wiping is the default policy. It erases the earliest results after 80 percent of the disk is used. When that threshold is reached, the system erases data to the 70 percent watermark.

Time-based wiping is configurable from 30 to 180 days.

Monitoring audit logs

Audit logs record all user activity on the McAfee DLP systems. Administrative permissions are required to view the logs.

Audit logs are located on the **User Administration** pages. The log elements can be rearranged by clicking headers, and the **Filter by** feature in the navigation pane can be used to sort the results.

Auditing live users

The Live Users feature records all activity in all live sessions. Administrator permissions are required to view the records.

Live user records are available on the **User Administration** | **Live Users** page. The **Session Id** links directly to the records of the users who are logged in.

Audit log actions

All user actions are sorted into categories when they are logged.

Table 19-1 Summary of audit log actions

Category	Actions
Devices	View, add, edit, delete
Statistics	View, view details, view system logs, delete system logs
Alias	Create, modify, delete alias; view alias list
Capture filters	Create, modify, delete, update, apply capture filters; view capture filter list; restore factory defaults
Configuration	Show, modify system configuration; modify IP management
Users and user groups	View, delete user audit logs; view user and use group accounts; add local and LDAP users; add, modify, delete, view, search for users; add, modify, delete user groups; view users group members and group lists
Permissions	View group, task, policy, user permissions; update user and task permissions; view, update failover setup
Servers	View, create, modify, delete, update DHCP and LDAP servers; add LDAP domain
Cases	View cases, view opening of cases
Policies/rules	Create, modify, delete, view policies; export/import policies and rules; view, download exported policies, rules, reports; view runtime, configuration of rules; view policy deployment status and error; view policy schedule
Search	Create, view, schedule, deschedule search; view search list, details, document, object; create document, email, FTP, image search; view search detail
Discover	Fetch, upload, attach file; show, cancel file upload
Summaries	View incident, user, location, risk, network, case summaries
Dashboard	Display, delete, save, create dashboard views; export dashboard
Incidents	Detect view incident annotations, history, attributes, matches; mark incident for deletion, as false positive, as read/unread
Reports	View, create, show reports and scheduled reports
Login	Log on, logout
Statistics/Results	View, delete, modify, who exports files/results, modify results per page
Utilities	View utilities, kernel version, system uptime, application version; show help, view status/version information; show disk capacity; display flow statistics

Generate audit log reports

Generate audit log reports to save them for future reference. Reports are saved in CSV (comma-separated values) format.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Audit Logs**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Audit Logs**.

2 Select **Actions** | **Export as CSV**.

3 Open or save the log.

If Microsoft Excel is installed and you select **Open**, the report will open in spreadsheet format.

Filter audit logs

Filter audit logs to troubleshoot systems that have been changed, or discover patterns in usage.

Click on the Session ID link of a user to see what actions the user has taken.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Audit Logs**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Audit Logs**.

2 Determine which cell in the audit log table will act as the primary key.

3 Click the cell to automatically create a filter in the **Filter by** pane.

The dashboard data immediately changes to reflect the selection.

4 Click **Clear All** in the **Filter by** pane before creating another filter.

Sort audit logs

Sort audit logs to rearrange the entries so that you can discover usage patterns or troubleshoot the system if it has been reconfigured.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **User Administration** | **Audit Logs**.
- On your McAfee DLP appliance, select **System** | **User Administration** | **Audit Logs**.

2 Determine which column in the audit log table will act as the primary key.

3 Click a column header to rearrange the log entries.

For example, you might select the **Timestamp** column header to find out what actions were taken in a specific time frame, or on the **User** column to find out who took those actions.

SNMP management

McAfee DLP appliances support Simple Network Management Protocol (SNMP), which is used to monitor the health of the appliance.

SNMP v2 and v3 are supported.

These properties can be monitored using SNMP traps for 4400 and 5500 appliances:

- Hard drive failure
- System fan or processor fan failure
- Memory usage exceeds the threshold
- CPU usage exceeds the threshold

- Power unit failure
- Disk usage exceeds the threshold
- System temperature exceeds the threshold

SNMP traps are not supported on 1650, 3650, or virtual appliances.

All McAfee DLP appliances can be monitored using SNMP queries. Standard Linux Object Identifiers (OIDs) are supported, such as uptime, CPU utilization, available system RAM, and interface statistics.

McAfee DLP Monitor capture interfaces cannot be monitored by SNMP queries.

Configure SNMP on 4400 or 5500 appliances

Configure SNMP trap settings in the user interface. Use the command line interface to enable SNMP queries.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
   - On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.

2 Select a device from the list and click **Configure**.

3 In the **SNMP Trap Configuration** section, complete the settings.

   If you are configuring SNMP v3 on multiple McAfee DLP appliances, you must specify a unique engine ID for each appliance.

4 Click **Update**.

5 Using a command line session, log on to the McAfee DLP appliance.

6 Configure /etc/snmp/snmpd.conf.

   For information on configuring snmpd.conf, see the man page:

   ```
   # man snmpd.conf
   ```

   If you are using SNMP v3, update the engine ID using the same value you specified in the user interface.

7 Enable snmpd to start at boot:

   a `# chkconfig --add snmpd`

   b `# chkconfig snmpd on`

8 Start snmpd:

   ```
   # service snmpd start
   ```

Configure SNMP on 1650, 3650, or virtual appliances

Use the command line interface to enable SNMP queries.

Task

1 Using a command line session, log on to the McAfee DLP appliance.

2 Configure /etc/snmp/snmpd.conf.

For information on configuring snmpd.conf, see the man page:

```
# man snmpd.conf
```

If you are using SNMP v3, update the engine ID setting in the configuration file. If you are configuring SNMP on multiple McAfee DLP appliances, you must specify a unique engine ID for each appliance.

3 Enable snmpd to start at boot:

- **1650 and 3650 appliances** — Enter:

  ```
  # chkconfig snmpd on
  ```

- **Virtual appliances** — Enter:

  ```
  # chkconfig --add snmpd

  # chkconfig snmpd on
  ```

4 Start snmpd:

```
# service snmpd start
```

Default SNMP v3 settings

By default, some SNMP v3 settings are preconfigured. Although these settings can be used for testing purposes, McAfee recommends you modify these settings when configuring SNMP for use in your network.

Table 19-2 Default SNMP v3 query settings

Setting	Value
Username	admin
Authentication Protocol	SHA
Authentication Password	dlppasswd
Privacy Protocol	AES256
Privacy Passphrase	dlppassphase

Table 19-3 Default SNMP v3 trap settings

Setting	Value
Username	trapadmin
Authentication Protocol	SHA
Authentication Password	dlptrappasswd
Privacy Protocol	AES256
Privacy Passphrase	dlptrapprivpass

Using network statistics

The **Network Statistics** page displays status information on all of the data captured on your McAfee DLP devices, including traffic and other relevant systems data. If you have system administrators' permissions, you can view this page and reconfigure the views to reveal significant patterns.

Network statistics are available only on **Data in Motion** devices — McAfee DLP Monitor and McAfee DLP Prevent.

Each of the statistical panes contains a different type of data, and clicking **Details** gives access to more granular results.

Example: You might want to know how much data one of your managed appliances captures in a specific period of time, how much *Yahoo_Chat* traffic there is on the network, or what percentage of the captured data consists of office documents. The graphical views on the page reveal answers to those questions and more at a glance.

Network statistics data captured is averaged over time and synchronized periodically. Updates are sent every 15 minutes from managed devices to McAfee DLP Manager.

Types of network statistics

Network statistics are generated as the data is collected, analyzed and displayed. They are useful for getting a comprehensive picture of your McAfee DLP systems.

Network statistics are summarized in three related analysis views:

- Protocol summary
- Content summary
- Source/Destination summary

Each view displays these statistics for the listed protocol, content type, source, or destination entries:

- **Size** — The total size in megabytes of all detected objects
- **Count** — The total number of detected objects
- **Incidents** — The total number of generated incidents, including matches from capture filters

The number of incidents reported on the dashboard might be different from the number of incidents reported in the network statistics view. Dashboard incidents do not include matches from capture filters.

Click **Details** in each header for more information.

Filtering network statistics

Network statistics can be filtered like any other data reported to McAfee DLP dashboards.

Use the **Filter by** and **Order by** menus to configure network statistics.

With the **Filter by** options, you can examine results on one or more registered devices within specific time ranges.

- Devices
- Time ranges

With the **Order by** menu, you can examine the results being returned from the systems within specific time ranges.

- Time Trend (Such as hourly or weekly)
- Counter Trend (Incidents, Size, Count)

Technical specifications

McAfee DLP appliances meet all safety and operational standards and are in compliance with FCC standards.

McAfee DLP rack mounting requirements

McAfee DLP hardware must be rack-mounted properly to ensure safe configuration.

Elevated operating ambient temperature

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment might be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the MAT (maximum ambient temperature) specified by the manufacturer.

Reduced air flow

Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical loading

Mounting of the equipment in the rack should be such that a hazardous condition is not created due to uneven mechanical loading.

Circuit overloading

Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable earthing

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (use of power strips).

McAfee DLP power redundancy

McAfee DLP appliances with more than one power supply must be configured to provide redundancy by sharing the load while operating at nominal power. Additional protection is provided if two electrical outlets that are on different circuit breakers are used.

Should one power supply fail, a back-up fan automatically turns on, an alarm sounds, and a warning light is illuminated. If this occurs, contact McAfee for a replacement unit.

If a McAfee DLP appliance loses power for any reason, it will not come back up unless you change the BIOS setting in advance. The motherboard is set to **off** by default.

McAfee DLP FCC compliance

McAfee DLP hardware has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 16 of the Federal Communications Commission rules. Any modifications to McAfee

DLP equipment, unless expressly approved by the party responsible for compliance, could void authority to operate the equipment.

Operation of the McAfee DLP appliances is subject to the following conditions:

- The device might cause harmful interference, and
- The device must accept any interference received, including interference that might cause unwanted operation.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

McAfee DLP equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instruction manual, it might cause harmful interference to radio communications. If operation of this equipment in a residential area causes harmful interference, it must be corrected at owner expense.

McAfee DLP safety compliance guidelines

McAfee DLP appliances must be operated in compliance within strict safety guidelines.

McAfee DLP hardware must be installed only in **Restricted Access** locations (dedicated equipment rooms, electrical closets, or the like).

Disconnect all power supply cords before servicing. There is a RISK OF EXPLOSION if a battery is replaced by an incorrect type. Dispose of used batteries according to industry standards.

20 Disaster recovery backup and restore

You can use the backup and restore feature to perform backups of your McAfee DLP system. Disaster recovery backups allow you to restore a McAfee DLP appliance to a previous operational state.

Contents

- *How the backup and restore process works*
- *Back up McAfee DLP systems*
- *Restore McAfee DLP systems*
- *Test a restored system*

How the backup and restore process works

When you back up a McAfee DLP system, an encrypted TAR archive is copied to an external storage server. This file can later be restored on the McAfee DLP appliance.

The backup process copies MySQL application databases to compressed archive files. The length of the backup process depends on the load on the system, size of the backup archive, and network latency. The archive file name contains the system's fully qualified domain name and a timestamp. The time stamp follows a yyyyMMdd-HHmm format.

Example: 20121030-1346 indicates this backup was completed at 1:46 p.m. on October 30, 2012:

```
manager.example.net-imanager-20121030-1346.tgz
```

For accurate timestamps, make sure your McAfee DLP appliance has the correct system time and is synchronized to an NTP server.

Use these options to control when to run a backup:

- Take an immediate backup.
- Schedule a one-time backup.
- Schedule a daily or weekly backup.

Backups are restored to the system by running a command line script.

What a backup contains

A backup file includes all policy and system configurations, but not all data is backed up.

A configuration backup includes these components:

- Policy configuration
- Local and Active Directory users
- Certificates and keys

- Scan settings
- User action logs
- Cases
- Incidents
- Endpoint configuration
- System settings
  - NTP
  - Syslog
  - SNMP
  - Time zone
  - Smart Host

These components are not included in a configuration backup:

- Capture data
- RSA keys on standalone devices
- Exported files, such as reports
- Reconnex File System (RFS)
- DNS configuration
- Management IP address

Backup and restore considerations

Depending on the features and components you use, there are some additional considerations for the backup and restore process.

Table 20-1 Backup and restore considerations

Component	Consideration
Product and version	A backup file must be restored to the same product and version.
Installation	A backup file must be restored on a new installation. For more information on installing software on an existing installation, see the *McAfee Data Loss Prevention Installation Guide*.
Managed devices	• Backup and restore is not supported on individual managed devices. Configuration and data from the managed devices are included in the McAfee DLP Manager backup. • If the backup file used to restore a McAfee DLP Manager system is not up to date, McAfee DLP devices might not share the configuration of the McAfee DLP Manager to which they are registered. If that happens, they might have to be unregistered and re-registered, and all incidents on the device will be deleted.
Disk space	The /data folder must not go over a certain percentage of used space: • **Model 4400 appliances** — less than 70 percent used • **Model 1650 and 3650 appliances** — less than 50 percent used The `df` command shows the percentage of used disk space.
Process timing	The backup and restore process depends on the volume of data on the appliance and the number of running and active scans. Processing time might be lengthy.
Communications between devices	Re-establishing communication channels between McAfee DLP Manager and managed devices might be lengthy depending on network connectivity.

Table 20-1 Backup and restore considerations *(continued)*

Component	Consideration
Policy match count	During a restore, the match count for all policies is reset to zero.
McAfee DLP Discover	When a scan is running, manifest information generated by the scan updates frequently. When a backup begins, scans are paused so that manifest information remains consistent. After the backup completes, any paused scans will resume running.
Capture filters	After a restore, the devices that filters are deployed on are reset, and must be redeployed.

Restoring on different hardware

A backup can be restored on the same type of hardware, but other migration paths exist.

Table 20-2 Options for restoring on different hardware

Backup appliance	Restore appliance
1650 and 3650	• 1650 • 3650 • 4400 • 5500 • Virtual installation
4400	• 4400 • 5500 • Virtual installation
5500	• 5500 • Virtual installation
Virtual installation	• 4400 • 5500 • Virtual installation

Different appliance models have different amounts of available disk space. When restoring on different hardware, make sure the /data partition on the target appliance has sufficient free space. Use the `df` command to show disk usage.

Back up McAfee DLP systems

Configure an immediate or scheduled backup or your McAfee DLP system.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Disaster Recovery Backup**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Disaster Recovery Backup**.

2 In the **Remote Host Name** field, enter the name of an external storage device such as a Microsoft Windows, Linux or UNIX server.

3 Enter the user name and password of a user that has read and write access to the remote system.

4 Select a **Share Type** option.

- **McAfee DLP Manager** — **CIFS** or **NFS**
- **Standalone devices** — **NFS**

5 Click **Browse** to select the directory that will receive the backup.

6 Define the port to be used to connect to the remote host.

The default port is 22. To change this, select the **advanced** checkbox and type the port number.

7 If you want to be notified of backup status, select one or more **Notification** checkboxes.

You can send notification to a specific address, or select one of the user group checkboxes to notify all members of a group.

8 Complete the backup.

- If you are running a one-time backup, click **Backup Now**.
- If you are scheduling a backup but starting it immediately, complete the **Schedule** section, then click **Backup Now**.

  Clicking **Backup Now** also saves the configuration.

- If you are scheduling a backup to run at a later time, complete the **Schedule** section, then click **Save**.

  Select the **None** button to cancel a backup schedule.

9 When the backup completes, the file name appears in the **Backup** table.

Click **Disaster Recovery Backup** if the file name does not appear after the backup completes.

Restore McAfee DLP systems

When you restore McAfee DLP databases, you must prepare the system, select a matching backup file, run the restore script, and test the restored system.

You cannot restore McAfee DLP appliances that are managed by McAfee Data Loss Prevention Manager.

Task

1 Install the McAfee DLP software that matches the version of the backup image. For more information on installing the software, see the *Install or upgrade the system* chapter.

Management interface and DNS configurations are not included in the backup. After installation, verify that the management interface and DNS are configured correctly.

2 Log on as root to the command line of the McAfee DLP appliance and run the restore script:

```
# /data/stingray/ksh/restore_system_data.ksh
```

Enter the required information when prompted.

a Type the IP address of the network share.

b Type the credentials needed to log on as root.

c Type the file name of the backup.

If validation completes, the backup image is restored, and the system restarts. If not, the script exits.

See also

Installing or upgrading the software on 1650 and 3650 appliances on page 50
Installing or upgrading the software on 4400 and 5500 appliances on page 45

Test a restored system

Test the McAfee DLP system to make sure the backup file restored properly.

Task

1 Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Reporting** | **Incidents**.
- On your McAfee DLP appliance, select **Incidents**.

Verify that all incidents are displayed.

From the **Filter by Timestamp** menu, select a time period in which you will recognize specific incidents. It might take some time for incidents to populate after a restore.

2 In the **Policies** tab, check the devices displayed in the **Deployed On** column.

3 Modify a policy or rule. If error messages appear, the McAfee DLP appliance is still completing the restore process.

4 [McAfee DLP Manager only] In the **System** tab, check the status of the managed devices.

5 In some cases, you might need to manually activate or clone a scan.

a Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Classify** | **Discover Scan Operations**.
- On your McAfee DLP appliance, select **Classify** | **Discover Scan Operations**.

b Select the scan.

c From the **Actions** menu, select **Activate**.

d To clone a scan, select the scan, then from the **Actions**, select **Clone**.

6 Redeploy capture filters.

a Select one of these options:

- In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sysconfig** | **System Administration** | **Capture Filters**.
- On your McAfee DLP appliance, select **System** | **System Administration** | **Capture Filters**.

b Use the **View** menu to select either **Network Capture Filter** or **Content Capture Filter**.

c Select the filter.

d From the **Devices** box, select the device on which you want to deploy the capture filter.

e Click **Save**.

21 Technical support

Before contacting McAfee technical support, create a technical support package.

Contents

- *Contact technical support*
- *Create a technical support package*

Contact technical support

Contact technical support by phone, email, or online.

Table 21-1 Technical support options

Technical support option	How to contact
Telephone	(800) 937-2237; (408) 988-3832
Support portal	mysupport.mcafee.com
Email	support@mcafee.com

Create a technical support package

Create a technical support package to give your technical support engineer the information needed to troubleshoot your McAfee DLP appliances.

Before you begin
You can download a technical support package and send it to McAfee support.

When you create a technical support package, a compressed tar file will be saved to the McAfee DLP appliance you are troubleshooting.

Task

1 Select one of these options:
   - In ePolicy Orchestrator, select **Menu** | **Data Loss Prevention** | **DLP Sys Config** | **System Administration** | **Devices**.
   - On your McAfee DLP appliance, select **System** | **System Administration** | **Devices**.
2 Select a McAfee DLP Monitor or McAfee DLP Discover system and click **More**.

   If you cannot see the link, expand your dashboard.
3 Click **Create tech support package**.
4 After a minute or two, click **Check back**.

5 Click **Save** to download the file to your desktop.

6 Email the file to your McAfee support representative.

Index

A

about this guide 13
action rules
    options 140
administrator accounts 81
Apple documents, searching for 297
application definitions, adding to rules 164
applications
    definitions 161
    list 159
attributes
    searching by 275
    sorting incidents by 241
audit logs
    actions 331
    filtering 332
    monitoring 330
    reports 331
    sorting 332
auditing 330, 331

B

backup 339
boot options 49

C

capture
    language support 132
    of archived files 268
capture filters
    changing deployment status 319
    cumulative effect 319
    deploying 318
    filtering by IP address 320
    modifying 320
    types 313
    viewing deployed filters 318
cases
    adding 258
    adding comments 262
    adding incidents 258
    credit card violations 265
    customizing columns 264
cases *(continued)*
    deleting 259
    deleting incidents 259
    exporting 259
    notifications 264
    notifying users 264
    ownership, changing 261
    prioritizing 261
    resolution status, changing 262
    status, changing 261
chat sessions, searching for 292
concepts
    applying to rules 122
    configuring 142
    deleting 122
    regular expression syntax 117
    restoring 122
    session 121
    types 117
configuration backup 339
content capture filters
    actions 314
    adding 316
    types 314
content concepts 117, 119, 278, 279
content types 129
conventions and icons used in this guide 13
credit card violations, case example 265
CSV reports 253

D

dashboards
    adding rows 249
    configuring columns 249
    customizing 249, 250
    display 249
    permissions 85
data patterns 243
data types 16
default application definitions 162
device class
    creating new 169
    status, changing 169
    types 168

device definitions
groups 170
plug and play 171
removable storage 170
device rules
Plug and Play 175
removable storage 174
types 173
devices
management 168
parameters, list of 176
plug and play 168, 172
removable storage 168
whitelisting 168
whitlisting 172
DHCP servers, adding 76
disaster recovery backup 339
distributed searches 267
document properties
options 142
document types, searching for 297
documentation
audience for this guide 13
product-specific, finding 14
typographical conventions and icons 13

E

email, searching for 288–291
encryption, of incidents 250
Enterprise Application List 159

F

failover accounts, configuring 82
file access 173, 175
files
searching by signature 295
searching by size 296
searching by type 296

G

geographic locations, searching for 310
GMT, in searches 307

H

history, of incidents 246
home page
customizing 240
permissions 240
HTML reports 252

I

images, searching for 299
incidents
adding to cases 258
attributes 246
case status 244
deleting 242
deleting from cases 259
filtering 242
getting details 244
reports 252
searching by geographic location 310
sorting 241
throttling 251
views 246, 248
installation
1650 appliances 51
3650 appliances 51
4400 appliances 46
5500 appliances 46
virtual 45
IP addresses
as capture filters 320
searching for 286, 287

K

keywords 275–277

L

local time, in searches 281
location-based tags 166
logical operators 274, 277
login settings 82
logos, adding to reports 254

M

management options 25
management port, connecting 44
match strings 245, 250
matching content with concepts 245
McAfee DLP Manager
adding McAfee DLP products 58, 328
initial configuration 55
McAfee DLP Prevent
configuring email servers 60
MTA server requirements 33
McAfee Endpoint Encryption 168
McAfee ServicePortal, accessing 14
Microsoft documents, searching for 297
Microsoft Office content, in searches 268
multiple search results 268

N

network capture filters
actions 314
adding 317

network capture filters *(continued)*
prioritizing 319
types 315
network ports, identifying 42
network tap 31, 32, 43
notifications
backup 341
cases 264
searches 273

O

office documents, searching for 298

P

parts of speech, exclusion in searches 269
password settings 82
PDF reports 252
permissions
checking 85
group incident 85
plug and play devices
device definitions 171
whitelisting 168
policy
options 139, 143
policy violations 241
ports
searching for 282
well-known 283
ports, default 34
pre-configured
dashboards 240
incident views 247
user groups 83
primary administrator accounts, configuring 81
proprietary documents, searching for 298

Q

queries*, See* searches

R

registered documents, configuring 143
regular expression syntax 117
relative time frame, in searches 281
removable storage devices 168
reports
adding logos 254
adding titles 254
generating 252
resolution status, of cases 262
restoring concepts 122
rules
applying concepts 122
file access 175
rules *(continued)*
options 140
Plug and Play 175
removable storage 174

S

scheduling reports 253
searches
by attribute 275
by content concepts 278
by content type 297, 298
by file creation time 281
by file modification time 282
by file type 296
by GMT 307
by keyword 275
by local time 281
by location 285
by port 282
by port range 282
by protocol 284
by relative time frame 281
by URL 285
case sensitivity 268
details 272
distributed 267
email 288–291
excluding content concepts in 279
excluding keywords 276
excluding ports in 283
excluding protocols in 284
exclusion of parts of speech 269
images 299
IP address 286, 287
keyword 276
language support 132
large scale 268
logical operators 274
multiple search results 268
negative 269
notification 273
proper names 269
setting parameters 271
stopping 272
tips 276
unsupported special characters 269
using templates 128
webmail 291, 292
with concept expressions 278
word stemming 270
ServicePortal, finding product documentation 14
session concepts 121
SNMP 332–334
source code, searching for 309

SPAN port 31, 32, 43
status, of cases 261

T

Technical Support, finding product information 14
templates
    adding 126
    amplifying queries 125
    configuring 141
    deleting 126
    description 125
    example 127
    removing from rules 127
    reviewing 125
    searching with 128
time filters 242

U

upgrade
    1650 appliances 52
    3650 appliances 52
upgrade *(continued)*
    4400 appliances 47
    5500 appliances 47
user accounts 81
user groups
    creating 83
    deleting 84

V

view vectors 247
virtual installation 45

W

web application definitions 165
webmail, searching for 291, 292
websites, searching by URL 285
whitelists
    application definitions 172
    plug and play devices 168, 172
word stemming 270